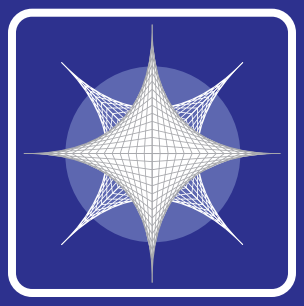


FORTINET

FortiOS™ Handbook - Fortinet Security Fabric

VERSION 6.0.2

FORTIOS VERSION 6.0

FORTINET DOCUMENT LIBRARY

https://docs.fortinet.com

FORTINET VIDEO GUIDE

https://video.fortinet.com

FORTINET KNOWLEDGE BASE

http://kb.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

http://cookbook.fortinet.com/how-to-work-with-fortinet-support/

FORTINET COOKBOOK

http://cookbook.fortinet.com

FORTINET TRAINING AND CERTIFICATION PROGRAM

https://www.fortinet.com/support-and-training/training.html

NSE INSTITUTE

https://training.fortinet.com/

FORTIGUARD CENTER

https://fortiguard.com

FORTICAST

http://forticast.fortinet.com

END USER LICENSE AGREEMENT

https://www.fortinet.com/doc/legal/EULA.pdf

July 26, 2018

FortiOS™ Handbook - Fortinet Security Fabric

01-602-481090-20180726

TABLE OF CONTENTS

Change log

Date	Change description
July 26, 2018	FortiOS 6.0.2 document release. See What's new in FortiOS 6.0.2.
July 6, 2018	Expanded Configuring Fabric Connectors.
June 5, 2018	FortiOS 6.0.1 document release. See What's new in FortiOS 6.0.1.
April 30, 2018	Added more information about FortiOS 6.0 features. See What's new in FortiOS 6.0.0.
March 29, 2018	FortiOS 6.0 document release. See What's new in FortiOS 6.0.0.

Introduction

The Fortinet Security Fabric is an end-to-end security solution that gives you control, integration, and easy management of security across your entire organization. The Security Fabric provides an intelligent architecture that interconnects discrete security solutions into an integrated whole to detect, monitor, block, and remediate attacks across the entire enterprise attack surface.

This document is a complete reference guide for the Security Fabric, including an overview of what the Security Fabric is, what devices are included in the Security Fabric and how they work together to secure your network, and how to configure and manage the Security Fabric.

What's new in FortiOS 6.0.2

The following list contains new Fortinet Security Fabric features added in FortiOS 6.0.2:

Automation features

- You can now test automation stitches in the GUI or by using the `diagnose automation test` command.
- When an automation stitch is triggered, the FortiGate creates an event log.

For more information, see "Automation stitches" on page 42.

Fabric Connector features

- FortiOS supports SDN Connectors to Google Cloud Platform (GCP).
- SDN Connectors to Amazon Web Services no longer require setting a VPC ID.
- SDN Connectors to Microsoft Azure no longer require setting an Azure subscription ID or Azure resource group.
- You can set the region for Azure to the Germany Azure Server or the US Government Azure Server.

For more information, see "Fabric Connectors" on page 55.

What's new in FortiOS 6.0.1

The following list contains new Fortinet Security Fabric features added in FortiOS 6.0.1:

New features

- Chaining and delaying actions for AWS Lambda and webhook
- Diagnose commands for automation stitches
- Available services for Fabric Connectors
- Verifying Fabric Connector status
- FortiManager in backup mode

6.0.1 GUI changes

- The options to configure single sign-on are now located at **Security Fabric > Fabric Connectors**.
- Automation stitches are available for FortiGate devices that don't belong to a Security Fabric.
- Two new triggers are available: **Security Rating Summary** and **AV & IPS DB Update**.
- The **Event Log** trigger now shows a list of events that can be used as triggers.
- The **FortiExplorer Notification** action now has warning and information message options.
- The **IOC level threshold** option is now called the **Threat level threshold**.
- The triggers for **Conserve Mode** and **High CPU** are now available only in the CLI.

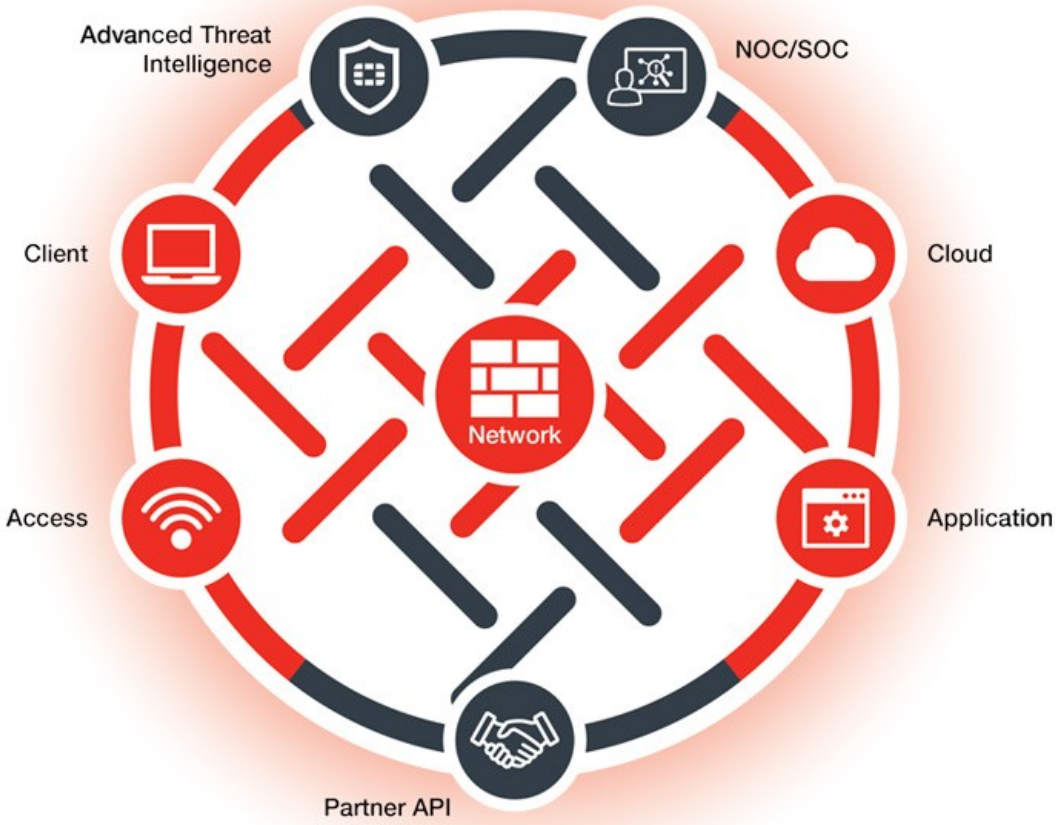
What's new in FortiOS 6.0.0

The following list contains new Fortinet Security Fabric features added in FortiOS 6.0:

- Automation stitches
- Security Fabric Rating license
- To authorize serial numbers of devices from the root FortiGate
- Joining the Security Fabric by device request
- For Physical and Logical Topology enhancements, see:
  - The WAN Cloud icon
  - Switch stacking
  - FortiAP and FortiSwitch integrations
  - Distinguishing client traffic from server traffic
  - Using the Search bar to find information in the topology views
- FortiMail Stats widget
- Desynchronizing the FortiAnalyzer, FortiSandbox, and FortiManager
- Fabric Connectors

Fortinet Security Fabric overview

The Fortinet Security Fabric provides a visionary approach to security that allows your organization to deliver intelligent, powerful, and seamless security. Fortinet offers security solutions for endpoints, access points, network elements, the data center, applications, cloud, and data, designed to work together as an integrated Security Fabric that can be integrated, analyzed, and managed to provide end-to-end protection for your network. Your organization can also add third-party products that are members of the Fabric-Ready Partner Program to the Security Fabric.



All elements in the Security Fabric work together as a team to share policy, threat intelligence, and application flow information. This collaborative approach expands network visibility and provides fast threat detection in real time and the ability to initiate and synchronize a coordinated response, no matter which part of the network is being compromised. The Security Fabric allows your network to automatically see and dynamically isolate affected devices, partition network segments, update rules, push out new policies, and remove malware.

The Security Fabric is designed to cover the entire attack surface and provide you with complete visibility into your network. It allows you to collect, share, and correlate threat intelligence between security and network devices,

centrally manage and orchestrate policies, automatically synchronize resources to enforce policies, and coordinate a response to threats detected anywhere across the extended network. The unified management interface provides you with cooperative security alerts, recommendations, audit reports, and full policy control across the Security Fabric that will give you confidence that your network is secure.

Access security

The Security Fabric secures the access layer of your organization's network. It integrates various access points in a network, such as endpoints, applications, the cloud, and IoT devices, regardless of their distribution, into an end-to-end solution that covers all attack surfaces.

Secure access architecture extends coordinated security policies to the edge of the wired and wireless network, where most vulnerabilities are targeted. It protects the access layer, guarding against data breaches and security threats from both internal user devices and IoT products.

Client security

Client security, through FortiClient, provides easy-to-manage, automated, fully customizable endpoint security for various devices. FortiClient provides end-to-end threat visibility and control by natively integrating endpoints into the security architecture and offers unified endpoint features, including compliance, protection, and secure access. It also offers integrated patch management and vulnerability shielding to harden all endpoints.

FortiClient integrates with the Security Fabric to provide real-time actionable visibility to stop threats to your organization's network at the endpoints.

For more information about FortiClient, see http://www.forticlient.com/.

Application security

The Security Fabric protects your organization's sensitive and proprietary data that is managed by applications, and ensures the security and availability of your organization's applications. It allows Fortinet application security products, and those of third-party vendors, to work together to boost security across core networks, remote devices, and the cloud. This provides your organization with a network architecture that is secure, aware, actionable, scalable, and open.

Fortinet's robust and integrated application security solution provides a complete end-to-end high-performance solution that protects your organization's valuable information by using a combination of Fortinet products which are deeply integrated into the Security Fabric for direct communications. These products include web application firewalls for application security, DDoS attack mitigation appliances for DDoS protection, advanced application delivery controllers (ADCs) to meet the demands of secure application traffic, sandboxing to isolate malicious code for inspection, and email security gateways that can detect and prevent email-borne threats from getting to your users.

Cloud security

The Security Fabric is designed to extend deep into different cloud environments to ensure that policies are consistent and enforced across all distributed resources. Within the unified security architecture, virtual firewalls can be deployed across private, public, and hybrid clouds to establish north-south and east-west microsegmentation. The Security Fabric weaves cloud applications into the broader environment, governed by seamless, universal security and compliance policies and managed using transparent visibility across the entire attack surface. Combining Fortinet Cloud Security with an existing enterprise firewall deployment extends the same powerful security, as well as the same intelligence and dynamic risk mitigation to applications located either in the cloud or on-premise.

NOC and SOC security

Fortinet's security operations center solution covers both IT and security risk management across your entire organization. The solution is a comprehensive approach to managing risk that includes adaptive awareness of the threat landscape, rapid local and global threat detection, reduced complexity in managing alerts and alarms, and reporting and analytics so you can better understand how your organization's risk profiles are being managed.

When Fortinet devices are unified into a Security Fabric, with compatible operating systems and shared intelligence, the security operations solution also includes information from network elements beyond Fortinet devices. The solution allows your network operations center (NOC) and security operations center (SOC) to share information, integrating and cross-correlating the data from each operations center. This additional context, visibility, and focus breaks down the barrier between your NOC and SOC, and gives you a comprehensive view across your entire Security Fabric so you can quickly find and respond to threats.

Advanced threat intelligence

Fortinet's Advanced Threat Protection (ATP) solution allows your organization to detect and mitigate against threats, both known and unknown, and share that information locally to deliver a coordinated defense.

The ATP solution relies on many types of security technologies, products, and research applied from the network edge through to endpoint devices. To deliver the most effective protection, they are integrated with other security elements from the Enterprise Firewall and Cloud solutions to work together automatically, continuously handing off data from one element to the next to identify, evaluate, and respond to attacks across the entire environment.

The ATP framework delivers end-to-end protection across the attack chain and consists of three elements: prevention, detection, and mitigation, with continuous threat monitoring and analytics from FortiGuard Labs.

For more information about the Advanced Threat Protection Solution, see http://www.fortinet.com/atp.

Partner API

The Fortinet Fabric-Ready Partner Program is an interoperability program for technology alliance partners. Technology alliance partners integrate their products with the Fortinet Security Fabric using Fortinet Security

Fabric APIs. Their products are then able to actively collect and share threat and mitigation information from one end of the security solution to the other, which improves threat intelligence, enhances overall threat awareness, and broadens threat response.

Inclusion in the program means that Fabric-Ready Partners have collaborated with Fortinet and leveraged the Fortinet Security Fabric APIs to develop and validate integrated end-to-end security solutions that are ready for deployment.

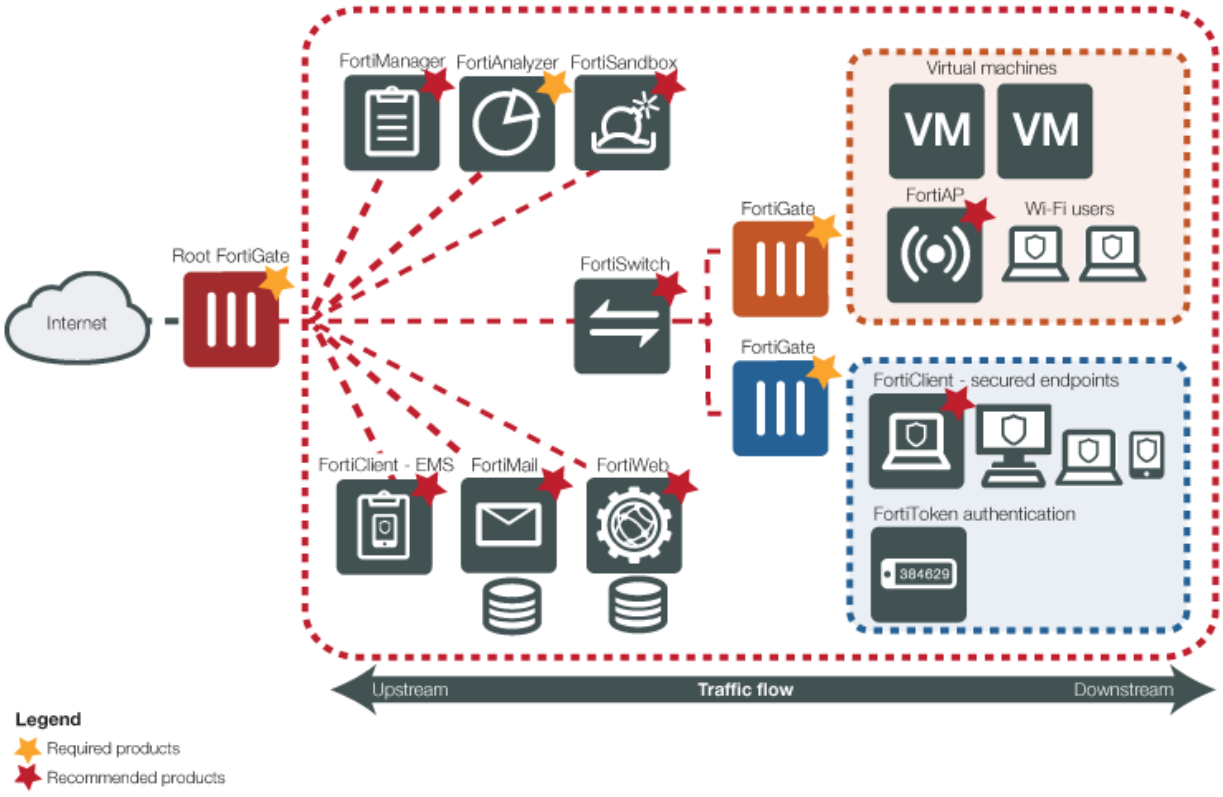
The Fabric-Ready Partner Program allows Fortinet technology alliance partners to build on Fortinet products and solutions which help your organization get even more value from your security deployment.

For more information about the Fortinet Fabric-Ready Partner Program, see

https://www.fortinet.com/partners/partnerships/alliance-partners.html

The Security Fabric solution components

The Fortinet Security Fabric consists of various components that work together to form the Security Fabric that secures your organization's network. The following diagram shows an example Security Fabric that contains both required and recommended Fortinet products:



Devices in the Security Fabric

The Security Fabric implementation consists of:

- Required devices
- Recommended devices
- Optional devices

Required devices

The following table shows devices that are required in the Fortinet Security Fabric:

Device	Description
FortiGate	FortiGate is a next-generation firewall (NGFW) that provides enterprise-class protection against network, content, and application-level threats. FortiGate devices are the core of the Security Fabric and can have one of the following roles in the Security Fabric: • **Root FortiGate**: The root FortiGate is the main component in the Security Fabric. It is typically located on the edge of the network and connects the internal devices and networks to the Internet through your ISP. From the root FortiGate, you can see information about the entire Security Fabric from the Physical and Logical Topology pages in the Security Fabric menu. • **Internal Segmentation Firewall (ISFW)**: After a root FortiGate is installed, all other FortiGate devices in the Security Fabric act as ISFWs. An ISFW is a firewall that is located at strategic points in your internal network, rather than on the network edge. This allows extra security measures to be taken around key network components, such as servers that contain valuable intellectual property. ISFW FortiGate devices create network visibility by sending traffic and information about the devices that are connected to them to the root FortiGate.
FortiAnalyzer	FortiAnalyzer collects, analyzes, and correlates log data from Fortinet devices throughout your organization's network, and allows you to view all firewall traffic and generate reports from a single console. FortiAnalyzer gives you increased visibility into your organization's network and simplifies network logging by storing and displaying all log information in one place. It provides centralized monitoring and awareness of threats, events, and network activity by collecting and correlating logs from Security Fabric devices, such as FortiGate, FortiClient, FortiSandbox, FortiWeb, and FortiMail. This gives you a deeper and more comprehensive view across your entire Security Fabric. You can use the robust security alert information and real-time threat intelligence that FortiAnalyzer provides to quickly identify and respond to security threats across your organization's network.

Recommended devices

The following table shows devices that Fortinet recommends you have in the Fortinet Security Fabric:

Device	Description
FortiAP	FortiAP is a wireless access point that provides integrated, secure, identity-driven wireless LAN access for your organization's network. You can add FortiAP devices to extend the Security Fabric to your wireless devices. Devices connected to a FortiAP appear in the Physical and Logical Topology pages in the Security Fabric menu.

Device	Description
FortiClient	FortiClient adds endpoint control to devices that are located in the Security Fabric, allowing only traffic from compliant devices to flow through the FortiGate. This is done through FortiClient compliance profiles. In the Security Fabric, FortiClient compliance profiles are applied by the first FortiGate that a device's traffic flows through. This is often an ISFW FortiGate. Device registration and on-net status information for a device that is running FortiClient appears only on the FortiGate that applies the FortiClient profile to the device.
FortiClient EMS	FortiClient Enterprise Management Server (EMS) is a security management solution that provides scalable and centralized management of multiple endpoint devices. FortiClient EMS is used in the Security Fabric to provide visibility across your network, to securely share information, and assign security profiles to endpoints.
FortiMail	FortiMail is a secure email gateway that uses various threat prevention methods, including antispam, antimalware, sandboxing, and anomaly detection. FortiMail integrates with other Fortinet products, as well as third-party virtual and cloud platforms, to help establish a seamless Security Fabric across the entire attack surface. FortiMail anti-spam processing helps offload other devices in the Security Fabric that would typically carry out this process.
FortiManager	FortiManager is an easy-to-use, single pane of glass management console, that gives you total visibility, full control, and complete protection of your organization's network. Using the FortiManager in the Security Fabric allows you to simplify the network management of devices in the Security Fabric by centralizing management access in a single device. This allows you to easily control the deployment of security policies, FortiGuard content security updates, firmware revisions, and individual configurations for devices in the Security Fabric.
FortiSandbox	FortiSandbox is an advanced threat protection appliance that improves your security architecture by identifying and validating threats in a separate, secure environment. You can add FortiSandbox to your Security Fabric to improve security with sandbox inspection. Sandbox integration allows FortiGate devices in the Security Fabric to automatically receive signature updates from FortiSandbox and add the originating URL of any malicious file to a blocked URL list.

Device	Description
FortiSwitch	FortiSwitch is a secure access switch that can be integrated into the Fortinet Security Fabric through the FortiLink protocol. FortiLink allows FortiSwitch ports to become logical extensions of the FortiGate. This allows the FortiGate to auto-discover a connected FortiSwitch for provisioning, including the attachment of policy to ports or VLANs. With an integrated access layer, the FortiGate provides consolidated visibility and reporting with Physical and Logical Topology views of the Security Fabric in the Security Fabric menu. You can add a FortiSwitch to the Security Fabric when it is managed by a FortiGate within the Security Fabric, and connected to an interface that uses FortiTelemetry. Devices connected to the FortiSwitch appear in the Physical and Logical Topology pages in the Security Fabric menu, and security features, such as FortiClient compliance profiles, are applied to them.
FortiWeb	FortiWeb is a web application firewall that protects hosted web applications from attacks that target known and unknown exploits. In the Security Fabric, FortiWeb defends the application attack surface from attacks that target application exploits. You can also configure FortiWeb to apply web application firewall features, virus scanning, and web filtering to HTTP traffic to help offload other devices in the Security Fabric that would typically carry out these processes.

Optional devices

The following table shows devices that are optional in the Fortinet Security Fabric:

Device	Description
Other Fortinet products	Many other Fortinet products can be added to the Security Fabric, including FortiAuthenticator, FortiToken, FortiCache, and FortiSIEM.
Third-party products	Third-party products that belong to the Fortinet Fabric-Ready Partner Program.

Security Fabric topology views

You can see the Security Fabric topology in the root FortiGate GUI. Two viewing options are available: the Physical Topology view and the Logical Topology view.

The Physical Topology view displays the physical structure of your network, by showing the devices in the Security Fabric and the connections between them. The Logical Topology view displays the logical structure of your network, by connection, by showing information about logical and physical network interfaces in the Security Fabric and the interfaces that connect devices in the Security Fabric. Only Fortinet devices are shown in the topology views.

For more information about the topology views, see "Using the Fortinet Security Fabric" on page 30.

Security Fabric Rating

The Security Fabric Rating provides a method to continually monitor and improve your organization's Security Fabric configuration. The Security Fabric Rating is a feature on the FortiGate that analyzes your Security Fabric deployment, identifies potential vulnerabilities, and highlights best practices that you can use to improve the overall security and performance of your network.

Using the Security Fabric Rating helps you to:

- Tune your network configuration
- Deploy new hardware and software
- Have more visibility into your network
- Gain more control over your network
- Adhere to your organization's compliance requirements

The Security Fabric Rating provides a Security Fabric Score based on how many security checks your network passes and fails during the test. By checking the Security Fabric Score, and implementing the recommendations, you can have confidence that your network is getting more secure over time.

For more information about running a Security Fabric Rating check, see "Using the Fortinet Security Fabric" on page 30.

FortiTelemetry

FortiTelemetry is a protocol that Fortinet products in the Security Fabric use to communicate with each other. It connects Security Fabric devices and allows dynamic status updates to travel between them. The Security Fabric uses FortiTelemetry to link various security sensors and tools together to collect, coordinate, and respond to malicious behavior anywhere it occurs in your network in real time.

You must enable FortiTelemetry on interfaces that connect Fortinet devices in the Security Fabric.

Configuring the Fortinet Security Fabric

This section contains information about how to configure a Fortinet Security Fabric:

- Forming the Security Fabric
- Setting up data collection with FortiAnalyzer
- Adding a FortiSandbox to the Security Fabric
- Adding a FortiManager to the Security Fabric
- Adding FortiClient EMS to the Security Fabric

System requirements

To set up the Security Fabric in FortiOS 6.0, the devices that you want to include in the Security Fabric must meet the Product Integration and Support requirements in the FortiOS Release Notes.

Some features of the Security Fabric are available only in certain firmware versions and models. Not all FortiGate models can run the FortiGuard Security Rating Service if they are the root FortiGate in a Security Fabric. For more information, see the Special Notices in the FortiOS Release Notes.

For more information about upgrading the Security Fabric to version 6.0, see the Fortinet Security Fabric Upgrade guide.

Prerequisites

- Determine which devices you want to have in the Security Fabric.
- Ensure devices meet the Configuring the Fortinet Security Fabric
- If devices are not already installed in your network, complete basic installation and configuration tasks by following the instructions in the device documentation.
- Disable virtual domains (VDOMs) on all FortiGate devices that you want to add to the Security Fabric.
- Configure all FortiGate devices that you want to add to the Security Fabric to use NAT/route mode.

Forming the Security Fabric

To form the Security Fabric, you configure the root FortiGate and then the ISFW FortiGate devices. Although you can configure any of the FortiGate devices in the Security Fabric to be the root FortiGate, you typically configure the edge FortiGate as the root FortiGate. This setup allows you to view the full topology of the Security Fabric from the top down.

The following procedures include configuration steps for a typical Security Fabric implementation, where the root FortiGate is the edge FortiGate and the ISFW FortiGate devices are all FortiGate devices that are downstream from the root FortiGate.

Adding devices to the Security Fabric

You can easily and securely allow FortiGate, FortiAP and FortiSwitch to join the Security Fabric without sharing the password of the root FortiGate. You can authorize these device serial numbers from the root FortiGate or

allow the device to join by request. New authorization requests include the serial number of the device, the device IP address, and a list of High Availability (HA) members.

HA members can contain up to four serial numbers and this list is used to ensure that, in the event of failover, the secondary FortiGate is still authorized.

After a FortiGate or FortiWiFi joins the Security Fabric, any connected FortiAP or FortiSwitch automatically appears in the topology. You can then authorize these additional devices from the FortiGate or FortiWiFi they're connected to or the root FortiGate.

To authorize serial numbers of devices from the root FortiGate

When you add the serial number of a Fortinet device to the trusted list on the root FortiGate, the device can join the Security Fabric as soon as it connects. After you authorize the new FortiGate, additional connected FortiAP and FortiSwitch devices automatically appear in the topology tree. From the topology tree, it's easier for you to authorize them with one click.

To authorize a FortiGate or a FortiWiFi from the root FortiGate:

1. Connect to the root FortiGate. To add the serial number of the new FortiGate to the Security Fabric trusted list, enter the following commands:

```
config system csf
   config trusted-list
      edit <serial-number>
   end
end
```

2. To enable FortiTelemetry on an interface, go to **Network > Interfaces** and edit the interface that connects to the FortiGate or FortiWiFi you are authorizing. Under Administrative Access, enable **FortiTelemetry**. For best practices, under Networked Devices, you can also enable **Device Detection**.
3. Connect to the FortiGate you're adding to the Security Fabric and set the following settings on the **Security Fabric > Settings** page:

FortiGate Telemetry	Enable **FortiGate Telemetry**.
Group name	Set the **Group name** to the same Security Fabric group name that's configured on the root FortiGate.
Group password	Leave this field blank.
Connect to upstream FortiGate	Enable **Connect to upstream FortiGate**.
FortiGate IP	Enter the IP address of the root FortiGate or upstream FortiGate you're connecting to.
Apply	Select **Apply**.

4. Connect to the root FortiGate. Open the **Security Fabric > Settings** page and verify that the FortiGate that you added appears in the Security Fabric Topology.

Joining the Security Fabric by device request

Your device can request to join the Security Fabric from another FortiGate. However, you must have the group name and the IP address of the root FortiGate. The administrator of the root FortiGate in the Security Fabric must also authorize your device before it can join the Security Fabric.

The root FortiGate must already have FortiTelemetry enabled on the interface that the device is connecting to.

To enable FortiTelemetry on an interface, go to **Network > Interfaces** and edit the interface that connects to the FortiGate or FortiWiFi you are authorizing. Under Administrative Access, enable **FortiTelemetry**. For best practices, under Networked Devices, you can also enable **Device Detection**.

To join the Security Fabric by device request - GUI:

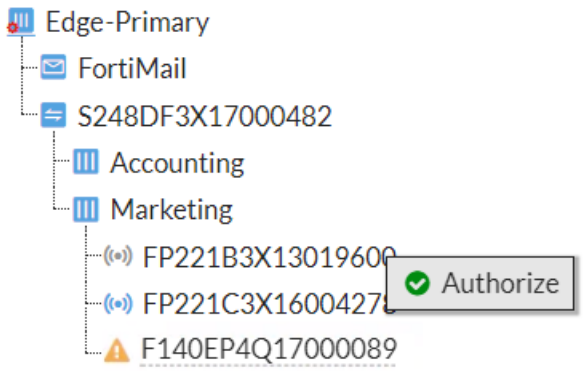
1. Connect to the unauthorized FortiGate or FortiWiFi, and go to **Security Fabric > Settings**.
2. From the Security Fabric Settings page, enable **FortiGate Telemetry**.
3. Enter the group name in the **Group name** field.
4. Leave the **Group password** blank.
5. To connect, enable **Connect to upstream FortiGate**.
6. Set the **FortiGate IP** to the IP address of the root FortiGate or upstream FortiGate that you want to connect to, and select **Apply**.
7. Connect to the root FortiGate and verify that the unauthorized FortiGate appears in the topology tree in **Security Fabric > Settings**. Hover over the unauthorized FortiGate and the tool tip shows the **Status** as **Waiting for Authorization**.
8. To authorize, click on the unauthorized FortiGate and select **Authorize**.

You can also allow other Fortinet devices to join the Security Fabric. You can authorize both FortiAP and FortiSwitch in the Security Fabric with one click. When you connect a FortiAP or FortiSwitch to an authorized FortiGate or FortiWiFi, the device automatically appears in the topology tree.

To authorize FortiAP and FortiSwitch devices

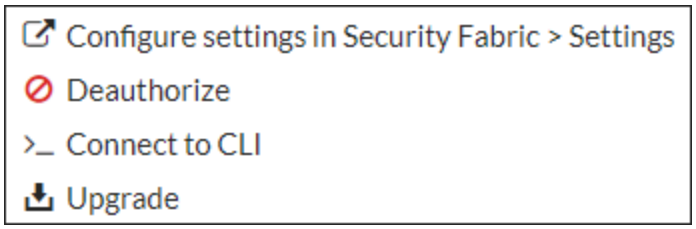
1. The topology tree is in the Security Fabric Settings page and in the Security Fabric Status widget on the Dashboard page. From either widget, click on the grayed out device icon to authorize or deauthorize it. Authorized devices turn blue and unauthorized products disappear from the topology tree.
2. Connect to the upstream FortiGate that the FortiAP or FortiSwitch is connected to.

The image below shows an unauthorized FortiAP in the topology widget:



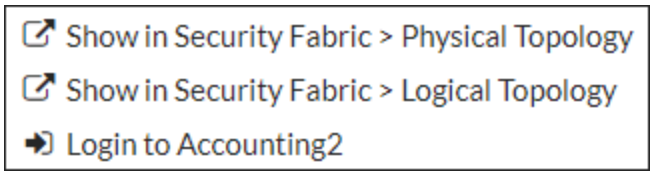
Note: You can also deauthorize FortiMail from the topology tree, however you must initially authorize FortiMail in the **Security Fabric > Settings** menu.

The following image shows FortiMail options:



Note: You can't authorize or deauthorize a FortiGate from the topology tree widget. You must disable FortiGate telemetry from the FortiGate you wish to deauthorize, or set the serial number to deny on the root FortiGate to remove it from the Security Fabric topology tree.

The following image shows FortiGate options:



Deauthorizing a device

You can deauthorize a device to remove it from the topology tree widget in the Security Fabric Settings page and in the Security Fabric Dashboard.

To deauthorize a FortiGate or FortiWiFi from the root FortiGate - GUI:

1. Connect to the root FortiGate.
2. To deauthorize the serial number of a trusted FortiGate or FortiWiFi, enter the following CLI commands:

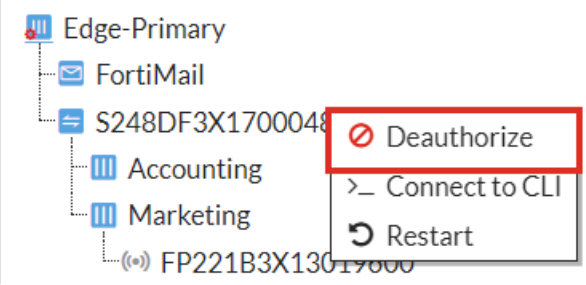
```
config system csf
   ...
   config trusted-list
        edit <serial-number>
           set action deny
   end
end
```

To leave the Security Fabric from a downstream FortiGate or FortiWiFi

1. Connect to the FortiGate or FortiWiFi that you want to deauthorize, and go to **Security Fabric > Settings**.
2. Disable **FortiGate Telemetry**.
3. **Apply** your changes.

To deauthorize a FortiSwitch, FortiAP, or FortiMail - GUI:

1. Connect to the upstream FortiGate and go to **Security Fabric > Settings** to see the topology. Alternatively, you can use the Security Fabric topology widget located in **Dashboard > Main**.
2. Click on the device and select **Deauthorize**. This removes the device from the topology tree.



After deauthorization, the serial numbers of the rejected device are saved in a trusted list that's available only in the CLI. You can view the trusted list using the `show system csf` command. The following example shows how the deauthorized FortiSwitch (from the image above) appears in the `trusted-list` with the action set to deny.

Syntax

```
show system csf
   config system csf
      set status enable
      set group-name "Office-Security-Fabric"
      set group-password ENC 1Z2X345V678
      config trusted-list
         edit "FGT6HD391806070"
         next
         edit "S248DF3X17000482"
            set action deny
         next
      end
   end
```

Add FortiAnalyzer to the root FortiGate of the Security Fabric

1. In the root FortiGate GUI, select **Security Fabric** > **Settings**.
2. In the Security Fabric Settings page, enable **FortiGate Telemetry**.
3. **FortiAnalyzer Logging** is automatically enabled.
4. In the **IP address** field, enter the IP address of the FortiAnalyzer that you want the Security Fabric to send logs to. If you select **Test Connectivity**, and this is the first time that you are connecting the FortiGate to the FortiAnalyzer, you will receive an error message because the FortiGate has not yet been authorized on the FortiAnalyzer. You can configure this authorization when you configure the FortiAnalyzer.
5. In the **Upload option** field, select the option for how often you want the FortiGate to send logs to the FortiAnalyzer.
6. If you want log transmissions encrypted, enable the **Encrypt log transmission** option. The log transmissions are encrypted using SSL.
7. Select **Apply**.

Additional CLI commands

You can use the following diagnose commands to view pending authorization requests, accept or deny authorization requests, or troubleshoot commands.

To view pending authorization requests on the root FortiGate - CLI:

```
diagnose system csf authorization pending-list
```

To accept or deny authorization requests to join the Security Fabric - CLI:

```
diagnose system csfd authorization {accept | deny} <serial-number-value>
```

where `serial-number-value` is the serial number of the device that has sent an authorization request to join the Security Fabric.

To view downstream device information - CLI:

```
diagnose system csf downstream
```

Configure ISFW FortiGate devices for the Security Fabric

You must have the group password of the root FortiGate to configure ISFW FortiGate devices for the Security Fabric.

1. In the ISFW FortiGate GUI, select **Security Fabric** > **Settings**.
2. In the Security Fabric Settings page, enable **FortiGate Telemetry**.
3. In the **Group name** field, enter the group name that you set for the Security Fabric.
4. In the **Group password** field, enter the group password that you set for the Security Fabric.
5. Enable the **Connect to upstream FortiGate** option.
6. In the **FortiGate IP** field, enter the IP address of the port on the upstream FortiGate that this FortiGate connects to. Depending on your network topology, the upstream FortiGate is another ISFW FortiGate or the root FortiGate. The FortiAnalyzer setting is automatically enabled. Settings for the FortiAnalyzer will be retrieved when the ISFW FortiGate connects to the root FortiGate.
7. Select **Apply**.
8. Repeat this procedure on every ISFW in the Security Fabric.

Setting up data collection with FortiAnalyzer

To set up data collection for the Security Fabric, you enable device detection on ISFW FortiGate devices and then connect the FortiAnalyzer to the Security Fabric.

You enable device detection on the interfaces of the ISFW FortiGate devices where you want the devices attached to those interfaces added to the Security Fabric. Only devices detected on those interfaces are shown in the Security Fabric topology views.

Connecting the FortiAnalyzer to the Security Fabric allows the Security Fabric to show historical data for the Security Fabric topology and logs for the entire Security Fabric.

Enable device detection on ISFW FortiGate devices

1. In the ISFW FortiGate GUI, select **Network** > **Interfaces**.
2. Select the interface that you want to enable device detection on.
3. Select **Edit** and in the **Networked Devices** section, enable **Device Detection**.

4. Select **OK**.
5. Repeat this procedure for every interface that you want to enable device detection on.

Desynchronizing the FortiAnalyzer, FortiSandbox, and FortiManager

If you want to add devices manually, you can edit the **Source IP** for downstream FortiGate devices in the **Central Management** settings. The **Central Management** settings are located in **Security Fabric > Settings**. However, if you change the **Source IP**, you must change the log settings to `local`.

If you don't want to automatically synchronize the configurations for FortiAnalyzer, FortiSandbox, and FortiManager, you can change the default system settings of the Security Fabric to use local settings.

To use local system settings - CLI:

```
config system csf
     set configuration-sync local
end
```

Where you set the following variables:

Option	Description
`default`	Synchronizes the configuration for FortiAnalyzer, FortiSandbox, and Central Management to the root FortiGate.
`local`	Doesn't synchronize the configuration with the root FortiGate, and you must configure settings individually.

Connect the FortiAnalyzer to the Security Fabric

Ensure that all FortiGate devices in the Security Fabric are registered with the same FortiAnalyzer.

1. In the FortiAnalyzer GUI, select **System Settings** > **Network**.
2. Select **All Interfaces**.
3. Select the port that connects to the root FortiGate.
4. Select **Edit**.
5. In the **IP Address/Netmask** field, enter the IP address used for the Security Fabric configuration on the root FortiGate.
6. In the **Default Gateway** field, enter the IP address of the interface on the root FortiGate that the FortiAnalyzer connects to.
7. Select **OK**.
8. Select **System Settings** > **Device Manager**.
   The FortiGate devices are listed as **Unregistered**.
9. Select the root FortiGate and the ISFW FortiGate devices in the Security Fabric.
10. Select **+ Add Device**.
    The FortiGate devices are now listed as **Registered**.

A warning icon will appear beside the root FortiGate, because the FortiAnalyzer requires administrative access to the root FortiGate in the Security Fabric.

11. In the **Authentication** window, complete the **Admin User** and **Password** fields to authenticate the Security Fabric.
    After the FortiAnalyzer authenticates the Security Fabric, the FortiAnalyzer shows the full Security Fabric topology.

You can verify that the FortiAnalyzer configuration is successful by selecting **Security Fabric** > **Settings** on the root and ISFW FortiGate devices. The **Storage usage** field in the **FortiAnalyzer Logging** section should now show storage usage information.

It is recommended that you create a user account for the FortiAnalyzer.

Adding a FortiSandbox to the Security Fabric

The Security Fabric supports both FortiSandbox Appliance and FortiSandbox Cloud. To use FortiSandbox Cloud, you must first activate a FortiCloud account.

To use FortiSandbox in a Security Fabric, you connect the FortiSandbox to the Security Fabric and then configure an antivirus profile to send files to the FortiSandbox. You can also use sandbox inspection in web filtering and FortiClient compliance profiles.

Connect the FortiSandbox to the Security Fabric

You configure FortiSandbox settings on the root FortiGate in the Security Fabric. After you configure these settings, the root FortiGate pushes them to the other FortiGate devices in the Security Fabric.

1. On the root FortiGate, go to **Security Fabric > Settings**.
2. Enable **Sandbox Inspection**.
3. Select either **FortiSandbox Appliance** or **FortiSandbox Cloud**.
4. If you're using a FortiSandbox Appliance, set **Server** to the IP address for the FortiSandbox.
5. Select **Apply**.

To authorize the FortiSandbox appliance, configure the following:

1. On the FortiSandbox, go to **Scan Input > Device**.
2. Edit the root FortiGate.
3. Under **Permissions & Policies**, select **Authorized**.
4. Select **OK**.
5. Authorize the other FortiGate devices in the Security Fabric.

Configure antivirus profiles

1. Go to **Security Profiles > AntiVirus**.
2. Create a new profile, edit an existing profile, or clone and edit an existing profile.
3. Under **Inspection Options**, set **Send Files to FortiSandbox Appliance/Cloud for Inspection** to **All Supported Files**.

4. Enable **Use FortiSandbox Database**.
5. Select **OK**.

Configure web filter profiles

1. Go to **Security Profiles > Web Filter**.
2. Create a new profile, edit an existing profile, or clone and edit an existing profile.
3. Under **Static URL Filter**, enable **Block malicious URLs discovered by FortiSandbox**.
4. Select **OK**.

Configure FortiClient compliance profiles

1. Go to **Security Profiles > FortiClient Compliance Profiles**.
2. Create a new profile, edit an existing profile, or clone and edit an existing profile.
3. Enable **Security Posture Check**.
4. Enable **Realtime Protection** and **Scan with FortiSandbox**.
5. Select **OK**.

Adding a FortiManager to the Security Fabric

When you add a FortiManager to the root FortiGate in the Security Fabric, it automatically synchronizes with any connected Security Fabric devices that are downstream. To add FortiManager to the Security Fabric, you must configure central management on the root FortiGate. Once you configure these settings, the root FortiGate pushes them to the other FortiGate devices in the Security Fabric. The FortiManager must have Internet access.

The following steps also ensure that the FortiGate can receive antivirus and IPS updates and allow remote management through the FortiManager system or FortiCloud service. The FortiManager device provides remote management of a FortiGate over TCP port 541. You must enable the FortiGate management option so the FortiGate can accept management updates to firmware and FortiGuard services.

Registering a FortiGate ensures that it receives updates to FortiGuard services. It also gives you access to technical support. To register the FortiGate, visit the Fortinet Support website.

To add a FortiManager to the root FortiGate - GUI:

1. On the root FortiGate, go to **Security Fabric > Settings**.
2. Enable **Central Management**.
3. In the **Type** field, select **FortiManager**.
4. Enter the **IP/Domain Name** for the FortiManager.
5. Select **Apply**.
6. On the FortiManager, go to **Device Manager**. The FortiGate devices in the Security Fabric are listed as **Unregistered Devices**.
7. Select the FortiGate devices, then select **+Add**.
8. Select **OK**.

To configure the FortiGate - CLI:

```
config system central-management
   set type fortimanager
   set fmg {<IP_address> | <FQDN_address>}
end
```

For more information about using FortiManager, see "Central management with FortiManager" on page 61.

Adding FortiClient EMS to the Security Fabric

You can configure endpoint control for your Security Fabric using FortiClient Endpoint Management System (EMS).

If you disable the **FortiClient Endpoint Management System (EMS)** option found on the **Security Fabric > Settings** page, it deletes all previously configured EMS server entries.

To configure an EMS Server - GUI:

1. To enable endpoint control, go to **System > Feature Visibility** and under Security Features, enable **Endpoint Control**. The FortiClient Endpoint Management System (EMS) section appears in the **Security Fabric > Settings** page.
2. Go to **Security Fabric > Settings** and enable **FortiClient Endpoint Management System (EMS)**.
3. Select the **+** to add it and enter the following:

Name	Enter the name of the EMS server.
Address	Select the FortiClient EMS address from the drop-down menu or select the **+** to create a new IP address or hostname.
Serial Number	
REST API Calls	

You can add a maximum of 16 EMS Servers.

4. **Apply** your changes.

To configure endpoint control settings - CLI:

```
config endpoint-control settings
   set forticlient-ems-rest-api-call-timeout <value>
end
```

where the value is set between 500 to 30000 milliseconds (default of 5000).

To configure a FortiClient Enterprise Management server - CLI:

```
config endpoint-control forticlient-ems
```

```
    edit 1
       set address <firewall-address-name>
       set serial-number <FortiClient-EMS-serial-number>
       set listen-port <listen-port-number>
       set upload-port <upload-port-number>
       set rest-api-auth <FortiClient-EMS-REST-API-authentication>
    next
end
```

where the following values are set to:

Variable	Description
`listen-port-number`	Set the listening port between 1 and 65535. The default port is 8013.
`upload-port-number`	Set the uploading port between 1 and 65535. The default port is 8014.

To configure FortiClient registration synchronization settings - CLI:

```
config endpoint-control forticlient-registration-synch
   edit <default-name>
      config {forticlient-winmac-setting | forticlient-android-settings | forticlient-ios-
          settings}
   next
end
```

To configure FortiClient endpoint control profiles - CLI:

```
config endpoint-control profile
   edit <profile-name>
      config {forticlient-winmac-setting | forticlient-android-settings | forticlient-ios-
          settings}
      set forticlient-ems-entries <FortiClient-EMS-entry-name>
   next
end
```

For information about further information about FortiClient EMS, see the FortiClient EMS Administration Guide.

Troubleshooting

The following commands can be useful for testing FortiClient EMS settings, including: signing in or out of FortiClient EMS, quarantining clients using EMS REST API, and adding quarantine calls to the queue. For additional troubleshooting commands, see the FortiOS CLI Reference.

- `diagnose endpoint forticlient-ems-rest-api signin <FortiClient-EMS-entry-name>`
- `diagnose endpoint forticlient-ems-rest-api signout <FortiClient-EMS-entry-name>`
- `diagnose endpoint forticlient-ems-rest-api quarantine-by-ipv4 <ipv4> <FortiClient-EMS-entry-name>`
- `diagnose endpoint forticlient-ems-rest-api unquarantine-by-ipv4 <ipv4> <FortiClient-EMS-entry-name>`
- `diagnose endpoint forticlient-ems-rest-api queue-quarantine-ipv4 <ipv4-address> [,<ipv4-address>...]` **To add multiple entries, separate the entries by a comma (no spaces).**

- `diagnose endpoint forticlient-ems-rest-api queue-unquarantine-ipv4 <ipv4> [,<ipv4-address>...]` **To add multiple entries, separate the entries by a comma (no spaces).**
- `diagnose debug application fcnacd_ems <integer>`

Using the Fortinet Security Fabric

Once you set up the Security Fabric, there are various Security Fabric features that you can use to improve your network security, including the following:

- Understanding the Security Fabric dashboard widgets
- Viewing the Security Fabric topology
- Running a Security Fabric Rating
- Automation stitches

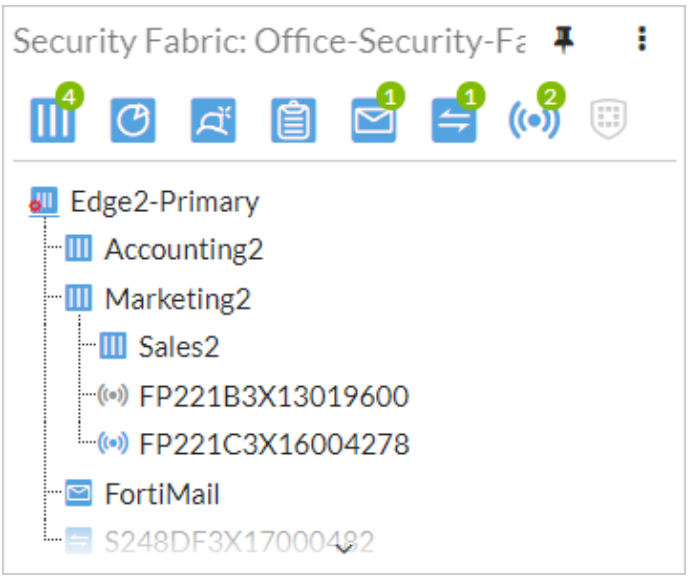
Understanding the Security Fabric dashboard widgets

You can add Security Fabric widgets to the dashboard on the root FortiGate. There are three widgets available: the Security Fabric Status widget, the Security Rating widget, and the FortiMail Statistics widget. The widgets allow you to see information about the status of the Security Fabric when you first log in to the FortiGate.

If any of these widgets do not appear on your dashboard, you can add them using the settings button in the bottom right corner. On the root FortiGate, select **Dashboard** > **Main** and the settings button appears when your mouse hovers over any part of the dashboard. Select **Add Widget** and under **Security Fabric**, click to add the widget.

The Security Fabric Status widget

The Security Fabric Status widget shows a visual summary of many of the devices in the Security Fabric. You can hover over the icons at the top of the widget to get a quick view of the status of the Security Fabric, including the status of FortiTelemetry and devices in the Security Fabric. You can click to authorize FortiAP and FortiSwitch devices that are connected to an authorized FortiGate.

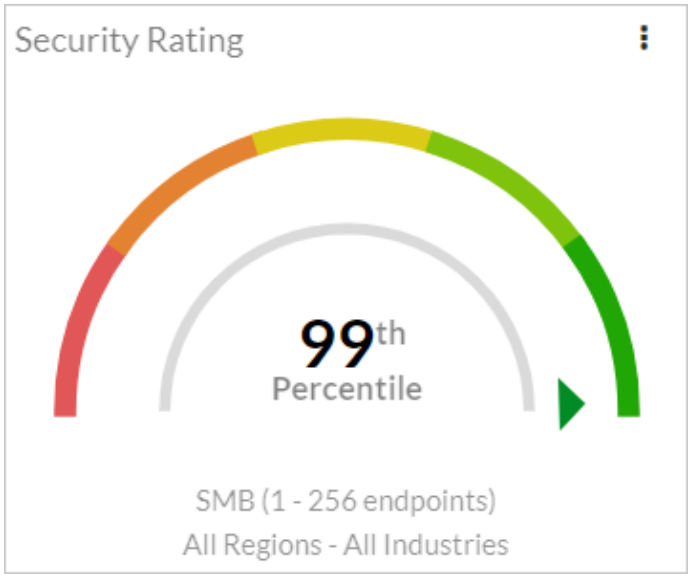


The widget shows the following information:

- The name of your Security Fabric
- Icons indicating the other Fortinet devices that can be used in the Security Fabric:
  - Devices in blue are connected in your network
  - Devices in gray are unauthorized devices that are connected in your network.
  - Devices in red are not detected in your network, but are recommended for the Security Fabric.
  - An attention icon shows a FortiGate or FortiWiFi waiting for Authorization.
- The names of the FortiGate devices in the Security Fabric

The Security Rating widget

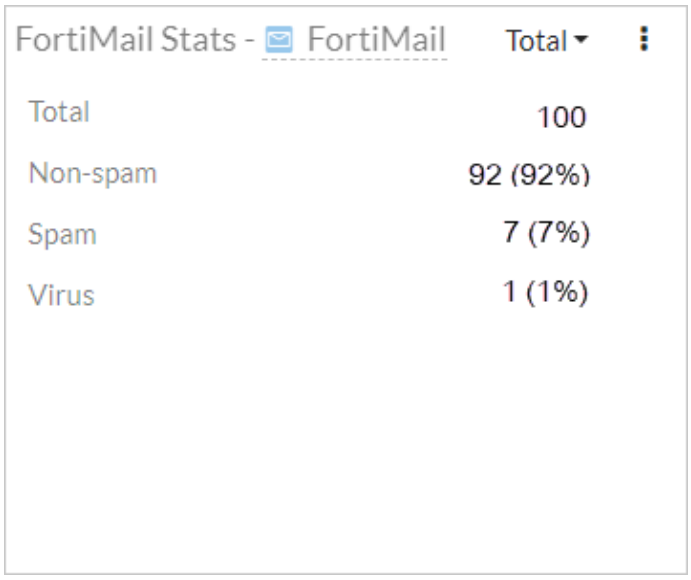
The Security Rating widget shows the latest Security Rating for your Security Fabric. You can configure the widget to show either how your organization's Security Fabric rating compares to the ratings of other organizations that belong to the same industry as your organization or all industries. Your organization's industry is determined from your FortiCare account. You can also configure the widget to either show scores that are specific to your organization's region or all regions. The widget shows the Security Rating score by percentile. To receive a Security Rating score, all FortiGate devices in the Security Fabric must have a valid Security Rating License.



FortiMail Stats widget

The FortiMail Stats widget shows mail detection statistics from FortiMail. You can configure the widget to show statistics from a FortiMail in your Security Fabric. If you have more than one FortiMail in your Security Fabric, you can add additional FortiMail Stats widgets to the Dashboard.

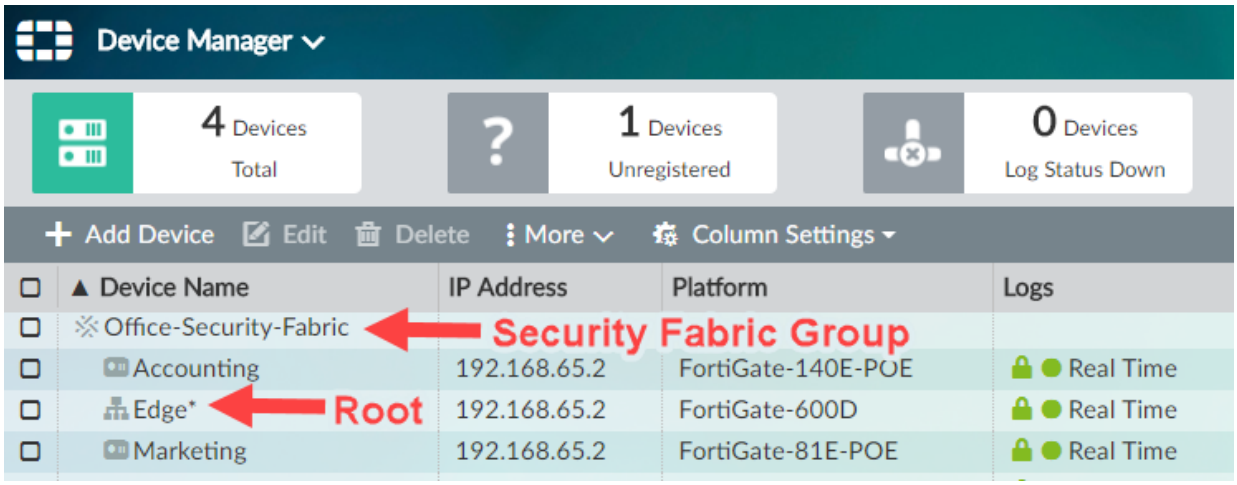
This widget shows both the total number and percentage of email messages that the FortiMail identifies as belonging to non-spam, spam, and virus categories. You can filter the statistics by time period, such as the number of messages per year, per month, and per hour.



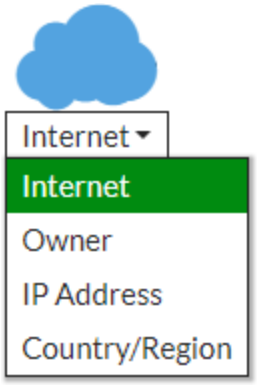
Viewing the Security Fabric topology

You can see the Security Fabric topology in the FortiGate GUI, in the Security Fabric menu. You can choose the Physical Topology or Logical Topology views. In both topology views, you can hover over device icons and use filtering and sorting options to see more information about devices and your organization's network. To view the complete network, you must access the topology views on the root FortiGate in the Security Fabric.

You can also see the Security Fabric topology in the FortiAnalyzer GUI. In the FortiAnalyzer GUI, select **Device Manager**. The FortiGate devices in the Security Fabric are shown as part of a Security Fabric group. An asterisk (*) appears beside the root FortiGate in the Security Fabric. To see the topology of the Security Fabric, right-click on the Security Fabric group and select **Fabric Topology**.Only Fortinet devices are shown in the Security Fabric topology views. The following image shows the FortiAnalyzer GUI.

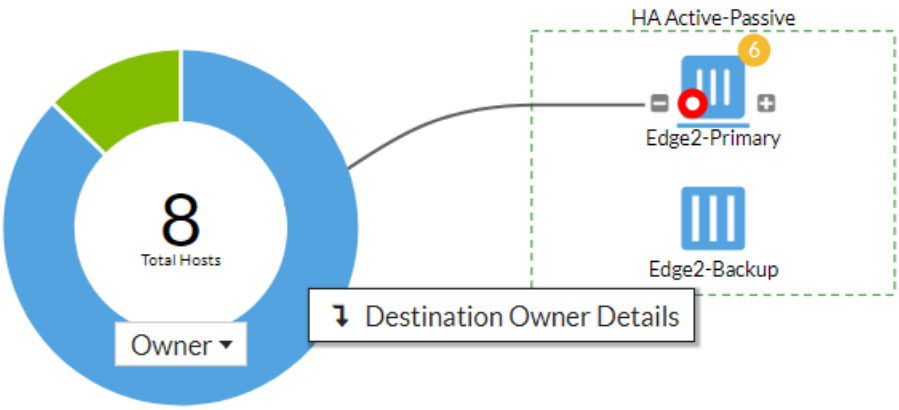


The WAN Cloud icon



The WAN cloud icon, in the Physical and Logical Topology views, allows you to receive destination data from the following options in the drop-down menu: Internet, owner IP address, and country/region. These options are available only in the Physical Topology view, when you select **Device Traffic** in the menu in the top right corner.

When you set the WAN cloud icon to **Owner**, the destination hosts are simplified to a fixed size donut chart. This chart shows the percentage division between Internal hosts (with private IP addresses) and Internet hosts. To see which color represents each host, hover over either color. To zoom in on the total number of hosts, click on the donut graph. To see more data for owner details in **FortiView > Destinations**, right-click and select **Destination Owner Details**. You can see the Internet Hosts in the screen shot below.

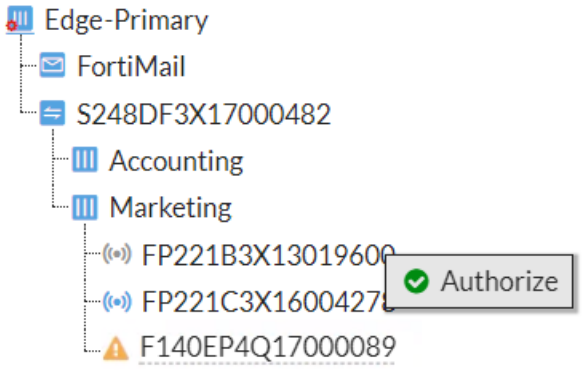


Switch stacking

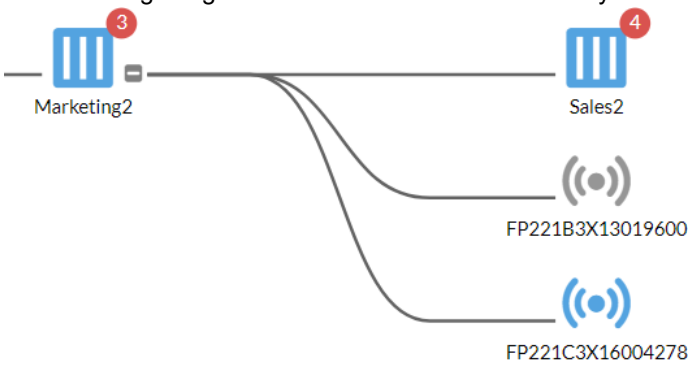
FortiAP and FortiSwitch links are enhanced in the Security Fabric's Logical and Topological views to show Link Aggregation Groups for the Inter-switch Link (ISL-LAG). This makes it easier to identify which links are physical links and which links are ISL-LAG. To quickly understand connectivity when you look at multiple link connections, ISL-LAG is identified with a thicker single line. To identify ISL-LAG groups with more than two links, you can also look at the port endpoint circles as references.

FortiAP and FortiSwitch integrations

You can see newly discovered FortiAP devices and FortiSwitches in the Security Fabric Topology widget as grayed-out icons, and you can click on any discovered device to authorize it. Once it's authorized, the device icon changes to blue. The following image shows the Security Fabric Topology widget.

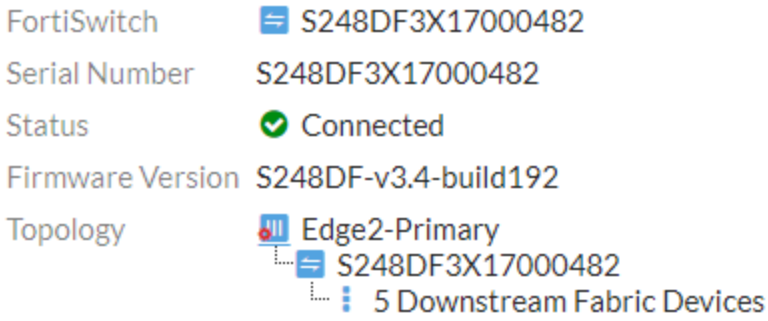


The following image shows the same device in the Physical and Logical Topology views.



For an authorized FortiAP, you can right-click to: either **Deauthorize** or **Restart the device**. For an authorized FortiSwitch, you can choose from the following management options: **Deauthorize**, **Connect to CLI**, **Restart** or **Upgrade**.

You can hover over the icon to show the device tooltips. Device tooltips show the connection status and firmware version. FortiSwitch also includes the faceplate and includes the physical port name and number of any devices connected to the FortiSwitch. The following image shows a FortiSwitch device tooltip.



Distinguishing client traffic from server traffic

The Physical and Logical Topology view shows servers and server clusters as rounded square shapes instead of bubbles, and they are grouped separately from endpoint devices to allow you to easily distinguish server traffic from other client traffic. Devices are grouped by device type. For example: Android phones, Apple phones, and Windows PCs.

Identifying compromised hosts from the topology views

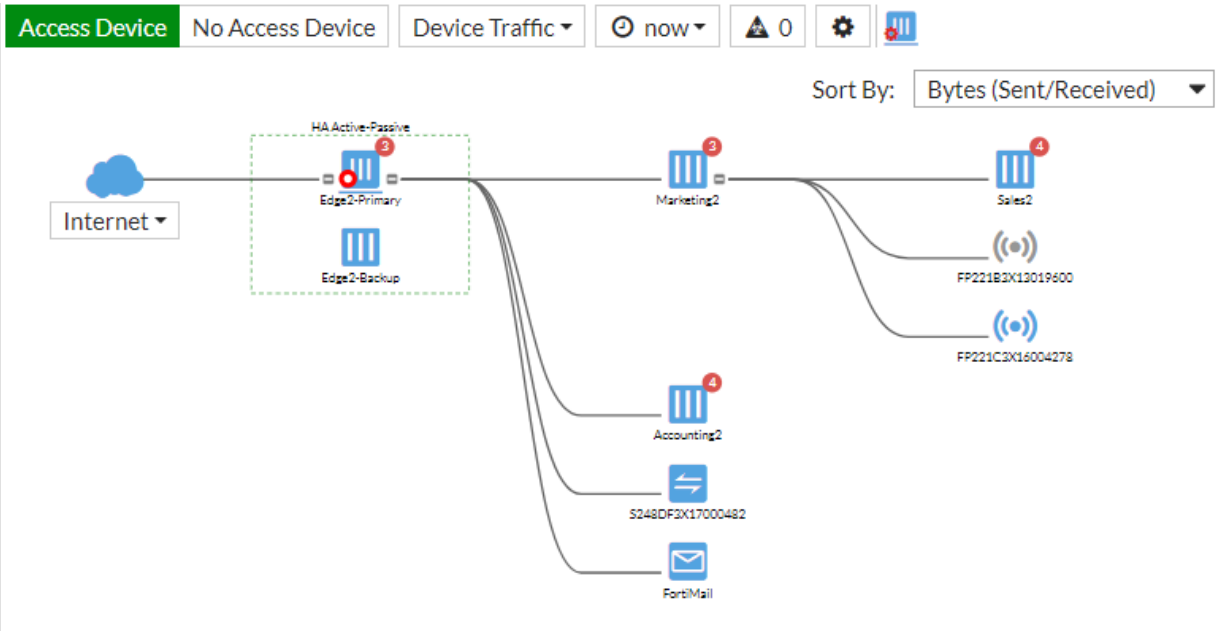
To view compromised hosts on your network and identify threats based on severity, you can click the Compromised Hosts icon in the Physical and Logical Topology views. To filter the compromised hosts by **Device Traffic**, **Device Count** or **IOC Score**, you must set the Bubble Option, located in the top-right corner. The host bubbles show different colors based on the IOC severity level. Confirmed threats appear in an actionable top-down list, located on the right side of the GUI, arranged based on threat severity.

The FortiAnalyzer in the Security Fabric retrieves the detected Indicators of Compromise (IOCs) from FortiGuard services. You can also view compromised host information in the FortiAnalyzer, in **FortiView > Threats > Compromised Hosts**.

View the Physical Topology

The Physical Topology view shows the devices in the Security Fabric and the devices they are connected to. You can also select whether or not to view access layer devices in this topology.

To see the Physical Topology, in the root FortiGate GUI, select **Security Fabric** > **Physical Topology**.



The Physical Topology view displays your network as a bubble chart of interconnected devices. These devices are grouped based on the upstream device they are connected to. The bubbles appear smaller or larger, based on their traffic volume. You can double-click any bubble to resize it and view more information about the device.

FortiGate devices and other networking devices are depicted as boxes. You can hover over the icon for each FortiGate to see information, such as serial number, hostname, and firmware version. You can hover over the bubbles of other devices to see information about them, such as name, IP address, and traffic volume data.

You can click the **Compromised Hosts** icon  , to view compromised hosts on your network and identify threats based on severity.

Security Fabric Rating recommendations are also shown in the topology, beside the icon of the device the recommendations apply to.

View the Logical Topology

The Logical Topology view is similar to the Physical Topology view, but it shows the network interfaces, logical or physical, that are used to connect devices in the Security Fabric.

To see the Logical Topology, in the root FortiGate GUI, select **Security Fabric** > **Logical Topology**.

The Logical Topology view displays your network as a bubble chart of network connection points. These devices are grouped based on the upstream device interface they are connected to. The bubbles appear smaller or larger, based on their traffic volume. You can double-click any bubble to re-size it.

FortiGate devices and other networking devices are depicted as boxes. You can hover over the icon for each FortiGate to see information, such as serial number, hostname, and firmware version. You can also see each FortiGate interface that has upstream and downstream devices connected to it. You can hover over the name of an interface to see its IP address, network (subnet), and role.

You can click the **Compromised Hosts** icon  , to view compromised hosts on your network and identify threats based on severity

Security Fabric Rating recommendations are also shown in the topology, beside the icon of the device the recommendations apply to.

Filter the topology views by specific criteria

You can use filters to narrow down the data on the topology views, so you can find specific information.

1. In the drop-down menu to the right of the **Search** field, select one of the following:
   - Device Traffic
   - Device Count
   - Device Type
   - Vulnerability
   - Threat Score
   - IOC Score
   - No Device
2. To filter the view by time, in the time period drop-down menu, select one of the following:
   - now
   - 5 minutes
   - 1 hour

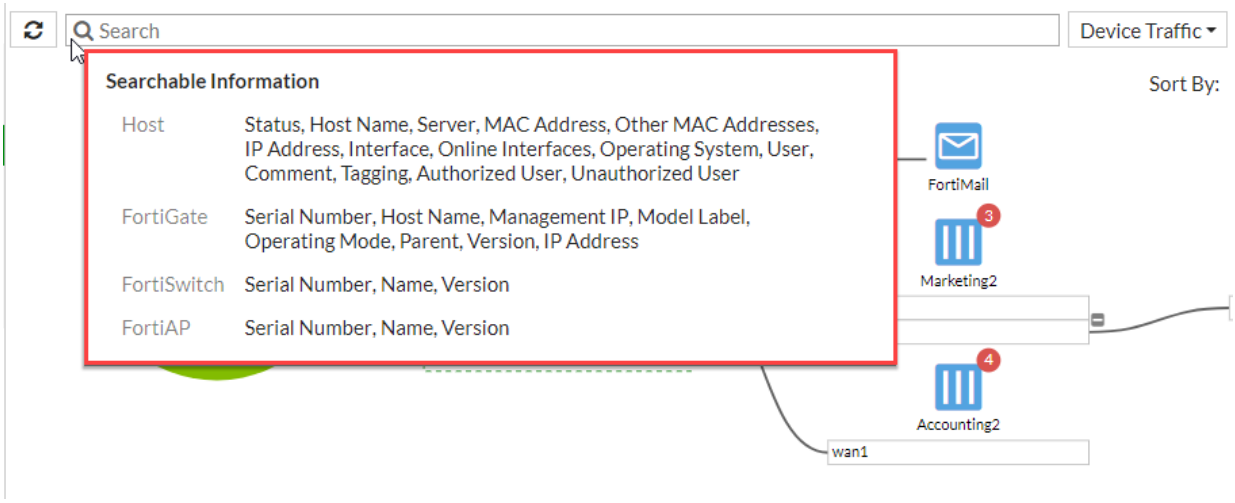
- 24 hours
- 7 days

3. To sort the topology by traffic options, in the **Sort By** drop-down menu, select one of the following:
   - Bytes (Sent/Received)
   - Packets (Sent/Received)
   - Bandwidth
   - Session

Using the Search bar to find information in the topology views

The search bar, located above the Physical and Logical Topology views, can help you easily find what you're looking for in the network topology and quickly resolve security issues. For example, you can search for unauthorized hosts and then decide which devices to authorize or remove from your network. The search highlights devices that match your search criteria, and grays out devices that don't match.

To see a list of items that you can search for, mouse over the search bar and a tooltip appears that shows **Searchable Information** list, organized by host and by Fortinet device type. The following image shows the search bar and the **Searchable Information** list:



For hosts, you can search for host information, such as status, host name, and server.

For FortiGate, you can search for device information, such as serial number, host name, and management IP address.

For FortiSwitch and FortiAP, you can search for device information, such as serial number, name and OS version.

Running a Security Fabric Rating

You can run a Security Fabric Rating to analyze your organization's Security Fabric deployment, identify potential vulnerabilities, and highlight best practices that you can use to improve the overall security and performance of your organization's network.

The Security Fabric Rating performs a variety of checks when it analyzes your network. All checks are based on your current network configuration, using real-time monitoring. The check runs across all FortiGate devices in the Security Fabric.

When the check is complete, a list of recommendations is shown. Two views are available: Failed or All Results. You can filter these views further in order to view results from a specific FortiGate or all FortiGate devices. Each view has a chart that shows the results of individual checks, and includes the name and a description of the check, which FortiGate the check was performed on, the impact of the check on the overall security score, and recommendations. If you hover over the result for a check, you can see a breakdown of how the score was determined.

You can choose to automatically apply the recommendations that include the Easy Apply option. By using Easy Apply, you can change the configuration of any FortiGate in the Security Fabric. Further action is required if you want to follow other recommendations.

You can also view recommendations for specific devices in the Physical and Logical Topology views in the Security Fabric menu. If a recommendation is available for a device, a circle containing a number appears. The number shows how many recommendations are available. The color of the circle shows the severity of the highest check that failed. The following table shows the severity that each color represents:

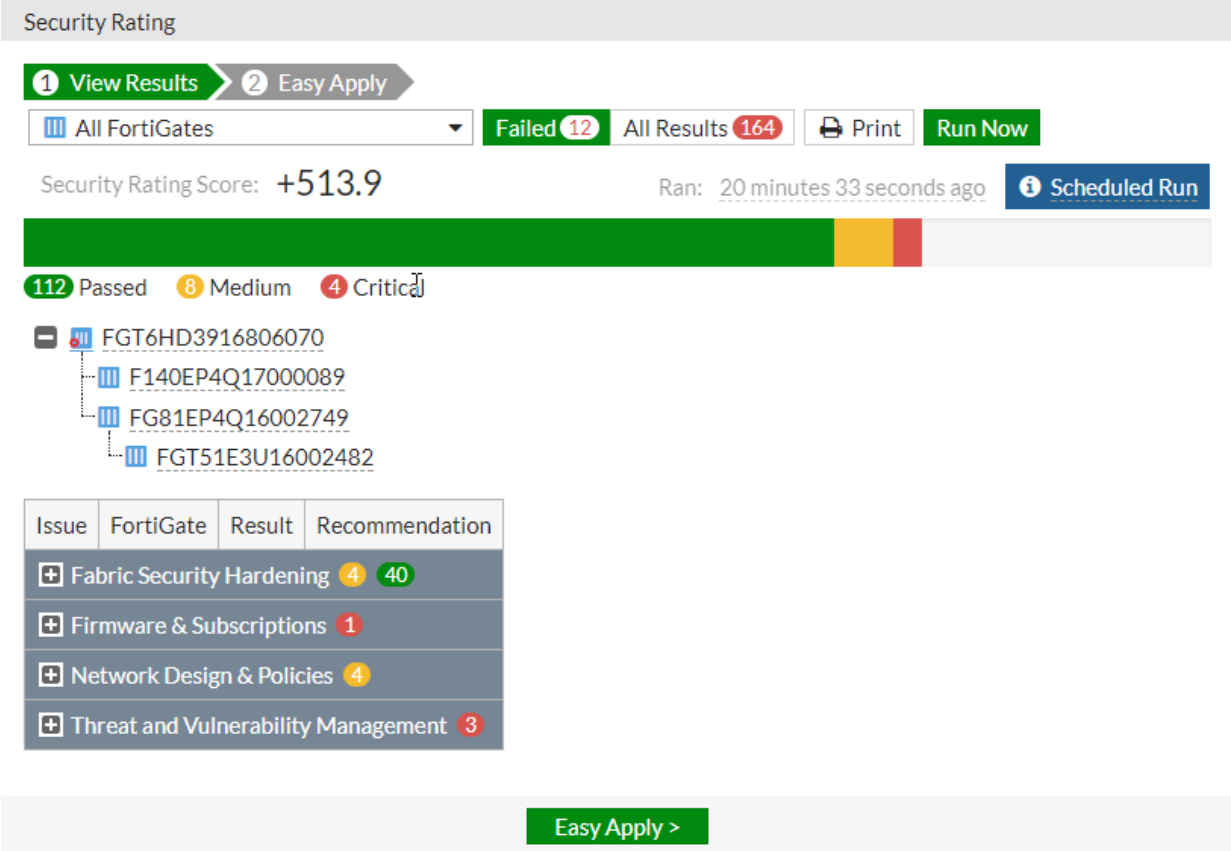
Color	Severity
Red	Critical
Orange	High
Yellow	Medium
Blue	Low

For more information about the Security Fabric Rating, and details about each of the checks that are performed, see the Fortinet Recommended Security Best Practices document.

Run a Security Fabric check

You must run the Security Fabric Rating check on the root FortiGate in the Security Fabric.

The following image shows the GUI:



1. In the root FortiGate GUI, select **Security Fabric** > **Security Rating**. Click **Show Topology** to view all FortiGate devices in the Security Fabric.
2. To run the check, select **Run Now**.
   The check will run. When it completes, it shows the following information:
   - The **Security Rating Score** field shows the score for your Security Fabric
   - The page shows the overall count of how many checks passed or failed, with the failed checks divided by severity
   - Information about each failed check, including which FortiGate failed the check, the effect of the check failure on the security score, and recommendations to fix the issue
   - The **Easy Apply** option appears with recommendations that can be automatically applied by the wizard
3. To move to the **Easy Apply** option page, select **Next**.
4. Select all recommendations that you want to implement in the Security Fabric.
5. Select **Apply Recommendations**.

Not all FortiGate models can run the FortiGuard Security Rating Service if they are the root FortiGate in a Security Fabric. For more information, see the FortiOS 6.0 Release Notes.

Security Fabric Rating license

The Security Rating license is a FortiGuard service and you must purchase a license to access to all the latest features. Security audit checks from FortiOS 5.6 will continue to run, but the following new upgrades are available only when you purchase a Security Rating license:

- Receive FortiGuard updates.
- Run Security Rating checks across each licensed device or all FortiGates in the Security Fabric from the Root FortiGate.
- New 6.0 Rating checks
- Submit rating scores to FortiGuard and receive Security Rating scores from FortiGuard for ranking customers by percentile.

For more information, see the Fortinet Recommended Security Best Practices document.

Opt out of customer ranking service

You can opt out of submitting Security Rating scores to FortiGuard.

If you opt out of from submitting your network's Security Rating scores, you won't be able to see how your organization's scores compare with the scores of other organizations. Instead, an absolute score is shown.

To disable FortiGuard Security Rating result submission - CLI:

```
config system global
      set fortiguard-audit-result-submission disable
   end
```

Logging for Security Fabric Rating

To view the results of past Security Fabric Rating checks, go to **Log & Report > Security Rating Events**.

You can also configure an event filter subtype for the Security Fabric Rating. When you run a check, event logs are created on the root FortiGate that summarize the results of the audit and show detailed information for the individual tests.

To configure logging for the Security Fabric Rating, use the following CLI commands:

```
config log eventfilter
   set security-audit enable
end
```

Understanding the Security Fabric Score

When you run a Security Fabric Rating, your organization's Security Fabric receives a Security Fabric Score. The score will be positive or negative, and a higher score represents a more secure network.

The score is based on how many checks your network passes and fails, as well as the severity level of these checks. The following table shows the weight for each severity level:

Severity level	Weight
Critical	50 points
High	25 points
Medium	10 points
Low	5 points

The check awards points when a check passes, using the following formula:

+ <Severity Weight> x *<Secure FortiGate Multiplier>*

where:

- *Severity Weight* is *<Severity level>* / *<number of FortiGate devices in the Security Fabric>*
- *Secure FortiGate Multiplier* is determined using logarithms and the number of FortiGate devices in the Security Fabric

For example, if you have four FortiGate devices in the Security Fabric, and all of them pass the Compatible Firmware check, the score for each FortiGate is calculated as: (50/4) x 1.292 = 16.2 points.

All FortiGate devices in the Security Fabric must pass the check in order to receive points. If any of the FortiGate devices in the Security Fabric fail a check, any FortiGate devices in the Security Fabric that passed the check are not awarded points. For the FortiGate that failed the test, the score is calculated using the following formula:

- <Severity Weight> x *<Count>*

where:

- *Severity Weight* is *<Severity level>*
- *Count* is the number of times the check failed during the check

For example, if the check finds two critical FortiClient vulnerabilities, the score for that check is calculated as: -50 x 2 = -100 points.

The score is not affected by checks that do not apply to your network. For example, if you do not have any FortiAP devices in the Security Fabric, you will not receive any points for the FortiAP Firmware Versions check.

Automation stitches

Automation stitches can be used for FortiGate devices that are not part of a Security Fabric.

Automation stitches allow you to decrease response times to security events by automating the activities between different device components in the Security Fabric. You can monitor events from any source in the Security Fabric and set up action responses to any destination.

This section includes:

Trigger events

You can configure FortiOS to automatically respond to the following trigger events: IOC, event log, reboot, conserve mode, high CPU, license expiry, HA failover, and configuration changes. The following table provides more information about the trigger event list.

Icon	Trigger	Description
	Compromised Host	An Indicator of compromise (IOC) is detected on a host endpoint. If you configure a **Compromised Host** trigger you also need to set the **IOC level** threshold to **Medium** or **High**. If you set this to **Medium**, both medium and high threshold attacks trigger an action. The additional **Action** options are the following: **Access Layer Quarantine, Quarantine FortiClient via EMS,** and **IP Ban**.

Icon	Trigger	Description
	Security Rating Summary	A summary is available for a recently run Security Rating.
	Configuration Change	There is a FortiGate configuration change.
	Reboot	A FortiGate reboot occurs.
	License Expiry	A FortiGuard license is expiring. You must select which type of license you want to be notified about if it expires: **FortiCare Support**, **FortiGuard Web Filter**, **FortiGuard AntiSpam**, **FortiGuard AntiVirus**, **FortiGuard IPS**, **FortiGuard Management Service**, and **FortiCloud**.
	HA Failover	HA failover occurs.
	AV & IPS DB Update	The antivirus and IPS database updates.

Icon	Trigger	Description
	Event Log	A FortiGate log with a specific event ID occurs. If you configure an **Event Log** trigger you'll also need to enter a **Log ID**.
CLI only	Conserve Mode	A FortiGate enters conserve mode due to low memory.
CLI only	High CPU	A FortiGate has high CPU usage.

Response actions

There are four main types of alert notifications you can set up to respond to an event trigger: **Email**, **FortiExplorer Notification**, **AWS Lambda**, and **Webhook**. There are also additional response actions for the Compromised Host (IOC): **Access Layer Quarantine, Quarantine FortiClient via EMS** and **IP ban**.

It's recommended that you set a **Minimum Interval** for each action. For more information, see "Avoiding repeat event notifications" on page 46.

Main Alert Notification Actions

Icon	Action	Description
	Email	Use this action to send a custom email notification. You must enter an email address and subject line.
	FortiExplorer Notification	Use this action to send push notifications to FortiExplorer. For the push to be successful, the FortiGate must be registered with FortiExplorer app on the iOS device you want to receive notifications on.

Icon	Action	Description
	AWS Lambda	Use this action to invoke Amazon Web Services (AWS) Lambda. For the **API Gateway** endpoint, you can manually enter the **URL** or you can enter the **Parameters** individually. For **URL**, you must enter the following variables: • Enter the **URL**. For example, "1a2b3c.execute-api.us-east-1.amazonaws.com/stagename/notification" • For **API Key**, enter the same API Key that you use for your AWS API Gateway. For **Parameters**, you must enter the following variables: • Set the **Region**. For example, "us-east-1" • Set the **ID** to the REST API ID. For example, "1a2b3c" • Set the **Path** to the resource you configured in your API Gateway. For example," notification". • Set the **Stage** to the stage name from your AWS API Gateway. For example, "stagename". • For the **API Key**, enter the same API key that you configured in your AWS API Gateway.
	Webhook	Use this action to send data to another application using a REST callback. You must enter the following: • For **Protocol** select **HTTP** or **HTTPS**. • For **Method** select **POST**, **PUT**, or **GET**. • Enter the **URI**. For example, "websitename.com/notifications" • Set the **Port**. • For **HTTP Body** enter the text you want (up to 1023 characters). For example, {"trigger":"reboot"}. • For HTTP Header, enter the **Name** and **Value** you want. For example, "x-notification-source" and "Fortinet".

Additional Compromised Host response actions

Icon	Action	Description
	Access Layer Quarantine	Use this action to impose a dynamic quarantine on multiple endpoints based on the access layer.

Icon	Action	Description
	Quarantine FortiClient via EMS	Use this action to use FortiClient EMS to block all traffic from the source addresses flagged as compromised hosts. Quarantined devices are flagged on the Security Fabric Physical and Logical topology views. Go to **Monitor > Quarantine Monitor** to view quarantined IP addresses. Addresses are automatically removed from the quarantine after a configurable period of time.
	IP Ban	Use this action to block all traffic from the source addresses flagged by the IOC. Go to **Monitor > Quarantine Monitor** to view banned IP addresses. Banned IP addresses can only be removed from the list by administrator intervention.

Avoiding repeat event notifications

The **Minimum interval** establishes the amount of time, in seconds, before you receive a repeat alert notification about the same event. This helps avoid receiving multiple alerts on your phone every few minutes for the same offense. When the interval has elapsed, a collated report detailing the activities during that time frame will be sent.

For example, if you were configuring an alert for high CPU usage, and you set the Minimum interval to 86400s (1 day) then you receive one alert when the CPU usage went above 90% and you would not get another alert notification for the same event until the next day. When the 86400s (1 day) elapses, you receive a notification with a summary that let's you know how many times the CPU usage exceeded 90% in the past day.

Creating automation stitches

To create an automation, you can set up a trigger event and response actions that cause the FortiOS to respond in a predetermined way. From the root FortiGate, you can set up triggers for event types, such as compromised host, high CPU, and configuration changes. The automation launches actions in response, such as email alerts, FortiExplorer notifications, and webhooks. The **Compromised Host** trigger has additional actions, such as access layer quarantine and quarantine FortiClient via EMS.

To create and test an automation - GUI:

1. Log in to the root FortiGate, and go to **Security Fabric > Automation**. Select **Create New**.
2. Customize the stitch by selecting a **Trigger** event type and the corresponding **Action** that you would like to automate. You can configure multiple actions for the same event trigger.
   Enter the following information:

Name	Enter a name for the new automation.

Status	Select **Enabled** to enable this automation.
FortiGate	From the drop-down menu, select the FortiGate device to apply this automation to or select **All FortiGates** (default) to apply to all.

Trigger	Select a **Trigger** from the following event types:
	• **Compromised Host**
	  • Set **IOC level threshold** to **Medium** or **High.**
	• **Event Log**
	  • Enter a **Log ID.**
	• **Reboot**
	• **Conserve Mode**
	• **High CPU**
	• **License Expiry**
	  • Set the **Licensetype** to one of the following: **FortiCare Support**, **FortiGuard Web Filter**, **FortiGuard AntiSpam**, **FortiGuard AntiVirus**, **FortiGuard IPS**, **FortiGuard Management Service**, or **FortiCloud**.
	• **HA Failover**
	• **Configuration Changes**

Action	If the **Trigger** event you select occurs, an alert is sent using the methods that you select here. Select at least one of the following **Action** types:
	• **Email**
	  • **Email subject**: Enter an email subject.
	  • **To:** Enter at least one email address. Select the plus **+** icon to add additional email addresses.
	• **FortiExplorer Notification**
	• **AWS Lambda**
	• **Webhook**
	
	NOTE: When you set the trigger to **Compromised Host**, the following Actions are available:
	• **Access Layer Quarantine**
	• **Quarantine FortiClient via EMS**
	• **IP Ban**

Minimum interval (seconds)	Enter a minimum time interval, in seconds, during which you won't receive repeated notifications for the same trigger occurrence. When the minimum time interval expires, you'll receive an alert with a compilation report of any events that occurred during the alloted interval period.

3. Select **OK**.
4. To test the new automation, right-click it and select **Test Automation Stitch**.

When an automation stitch is triggered, the FortiGate creates an event log, which you can view by going to **Log & Report > System Events**.

To create and test an automation - CLI:

```
config system automation-stitch
   edit <automation-stitch-name>
      set status {enable | disable}
      set trigger <trigger-name>
      set action <action-name>
      set destination <serial-number>
   next
end

diagnose automation test <automation-stitch-name> <log>
```

You can configure an automation using the `config system automation-stitch` command shown above. For more information about configuring the **Trigger**`<trigger-name>` and **Action**`<action-name>` components, see: "Configuring an automation, trigger, and action in the CLI" on page 48 .

Configuring an automation, trigger, and action in the CLI

This section provides instructions for how to create an automation, and expands on the CLI syntax shown in the introduction by explaining further details, including how to create both a trigger and an action.

To enable the Security Fabric - CLI:

```
config system csf
   set status enable
end
```

To create an "automation-stitch" - CLI:

```
config system automation-stitch
   edit <Automation-stitch-name>
      set status {enable | disable}
      set trigger <trigger-name>
      set action <action-name>
      set destination <serial-number>
   next
end
```

Where the following variables are set:

Variable	Description	Default
`edit <Automation-stitch-name>`	Enter the name of the new automation.	No default

Variable	Description	Default
`set status {enable | disable}`	Enter `enable` to enable the stitch.	Enable
`set trigger <trigger-name>`	Enter a trigger.	No default
`set action <action-name>`	Enter at least one action you want to occur when a trigger event or schedule occurs.	No default
`set destination <serial-number>`	The `destination` can be set to a list of device serial numbers, separated by spaces or left blank to use all members of the Security Fabric. Automation stitches are only applied to serial numbers listed in the destination.	All FortiGates

To create an "automation-action" - CLI:

```
config system automation-action
   edit <action-name>
      set action-type {email | ios-notification | alert | disable-ssid | quarantine |
          quarantine-forticlient | ban-ip | aws-lambda | webhook}
      set email-to <email-address>
      set email-subject <subject-name>
      set minimum-interval <seconds>
   next
end
```

Where the following variables are set:

Variable	Description	Default
`edit <Automation-action-name>`	Enter the name of the new automation action.	No default
`set action-type`	Select an action type from the following: email, ios-notification, alert, disable-ssid, quarantine, quarantine FortiClient, ban IP, AWS Lambda, and webhook.	No default
`set email-to <email-address>`	Enter the email address from which you would like to receive alert notifications. You can add multiple emails by selecting the **+** icon.	No default
`set email-subject <subject-name>`	Enter the email subject which you would like to see on your email notification alerts.	No default
`set minimum-interval`	Enter a minimal time interval between 0 to 2592000 seconds, during which a repeat offense of an action will be ignored to help avoid repeat alerts.	Default = 0 seconds

To create an "automation-trigger" - CLI:

```
config system automation-trigger
   edit <trigger-name>
      set trigger-type {event-based | scheduled}
      set event-type {ioc | event-log | reboot | low-memory | high-cpu | license-near-
          expiry | ha-failover | config-change}
      set ioc-level {medium | high}
      set logid [1-99999]
      set license-type {forticare-support | fortiguard-webfilter | fortiguard-antispam
          | fortiguard-antivirus | fortiguard-ips | fortiguard-management | forticloud
          | set trigger-frequency}
      set trigger-frequency {hourly | daily | weekly | monthly}
      set trigger-day <1-31>
      set trigger-hour <0-23>
      set trigger-minute <0-60>
   next
end
```

Where the following variables are set:

Variable	Description	Default
`edit <automation-trigger-name>`	Enter the name of the new trigger.	No default
`set event-type`	Select the event type from the following: • `ioc` • `event-log` • `reboot` • `low-memory` • `high-cpu` • `license-near-expiry` • `ha-failover` • `config-change`	No default
`set ioc-level`	Set the IOC level to `medium` or `high`. Where: • `medium` sends alerts for both medium and high IOC levels. • `high` only sends alerts for high IOC levels. **NOTE:** Only available when `event-type` is set to `ioc`.	No default
`set logid`	Log ID to trigger event. Value from **NOTE:** Only available when `event-type` is set to `event-log`.	No default

Variable	Description	Default
`set license-type`	Select the license type that you would like to be notified of in the event of expiry. The options include: • `forticare-support` (FortiCare support license) • `fortiguard-webfilter` (FortiGuard web filter license) • `fortiguard-antispam` (FortiGuard antispam license) • `fortiguard-antivirus` (FortiGuard AntiVirus license) • `fortiguard-ips` (FortiGuard IPS license) • `fortiguard-management` (FortiGuard management service license) • `forticloud` (FortiCloud license) **NOTE:** Only available when `event-type` is set to `license-near-expiry`.	No default
`set trigger-type`	Enter the trigger type as either `event-based` or `scheduled`.	No default
`set trigger-frequency`	How often the trigger is run. The options for the scheduled trigger frequency are the following: hourly, daily, weekly, or monthly. **NOTE:** Only available when `trigger-type` is set to `scheduled`.	Daily.
`set trigger-day`	Enter an integer value from 1 to 31. This is the day within the month to trigger.	No default
`set trigger-hour`	Enter the hour of the day on which to trigger from 0 to 23. **NOTE:** Only available when `trigger-type` is set to `scheduled`.	1
`set trigger-minute`	Enter the minute of the hour on which to trigger (0 - 59, 60 to randomize).	No default

Setting up an automation destination

The `config system automation-destination` command allows you to set the type to the primary FortiGate of an HA cluster or a single FortiGate, and both types of endpoint require it to be set to a destination [by serial number]. Then you can add the destination to any automation stitch. For more information on how to configure an HA cluster as the automation destination see the *High Availability Handbook*.

To set an automation destination:

```
config system automation-destination
   edit <name>
      set type {fortigate | ha-cluster}
      set destination <serial_number>
      set ha-group-id <number>
   next
```

Then you can add the destination to any automation stitch:

```
config system automation-stitch
   edit <stitch-name>
      set destination <destination-name>
end
```

Chaining and delaying actions for AWS Lambda and webhook

For automation stitches that use the action for **AWS Lambda** or **Webhook**, extra options are available to support chaining and delaying these actions. You can configure these options using the CLI.

To enable chaining actions by delaying an action until the previous action is finished, use the command `set required enable`. This option is only available when `action-type` is set to `aws-lambda` or `webhook`, and it's `disabled` by default.

To delay the execution of the action, use the command `set delay <seconds>`. This option is only available when `action-type` is set to `aws-lambda` or `webhook`, and it's set to 0 by default.

CLI syntax

```
config system automation-action
   edit <name>
      set action-type {aws-lambda | webhook}
      set required {enable | disable}
      set delay <seconds>
   next
end
```

Diagnose commands for automation stitches

Diagnose commands are available for automation stitches, allowing you to do the following:

- Test an automation stitch
- Enable and disable log dumping for automation stitches
- Display settings for every automation stitch
- Display history for every automation stitch

Test an automation stitch

To test an automation stitch, use the `diagnose automation test <automation-stitch-name> <log>` command.

Example output

```
# diagnose automation test HA-failover
automation test is done. stitch:HA-failover
```

Enable and disable log dumping for automation stitches

To toggle between enabling and disabling log dumping, use the `diagnose test application autod 1` command.

Example output

```
# diagnose test application autod 1
autod log dumping is enabled

# diagnose test application autod 1
autod log dumping is disabled

autod logs dumpping summary:
autod dumped total:0 logs, num of logids:0
```

Display settings for every automation stitch

To display settings for all automation stitches, use the `diagnose test application autod 2` command.

Example output

```
# diagnose test application autod 2
csf: enabled root:yes
total stitches activated: 2

stitch: Compromised-IP-Banned
destinations: all
trigger: Compromised-IP-Banned
actions:
Compromised-IP-Banned_ban-ip type:ban-ip interval:0


stitch: HA-failover
destinations: HA-failover_ha-cluster_25;
trigger: HA-failover
actions:
HA-failover_email type:email interval:0
subject: HA Failover
mailto:admin@example.com;
```

Display history for every automation stitch

To display the history for all your automation stitches, use the `diagnose test application autod 3` command.

Example output

```
# diagnose test application autod 3

stitch: Compromised-IP-Banned

local hit: 0 relayed to: 0 relayed from: 0
last trigger:Wed Dec 31 20:00:00 1969
last relay:Wed Dec 31 20:00:00 1969

actions:
Compromised-IP-Banned_ban-ip:
done: 0 relayed to: 0 relayed from: 0
last trigger:Wed Dec 31 20:00:00 1969
last relay:Wed Dec 31 20:00:00 1969


stitch: HA-failover

local hit: 1 relayed to: 1 relayed from: 1
last trigger:Thu May 24 11:35:22 2018
last relay:Thu May 24 11:35:22 2018

actions:
HA-failover_email:
done: 1 relayed to: 1 relayed from: 1
last trigger:Thu May 24 11:35:22 2018
last relay:Thu May 24 11:35:22 2018
```

Fabric Connectors

You can use Fabric Connectors for FortiGate devices that don't belong to a Security Fabric.

There are three types of Fabric Connectors, which allow you to connect your network to external services. The three types are: SDN, SSO/identity, and thread feeds.

This section contains the following information:

Available services for Fabric Connectors

Fabric Connectors support the following services:

SDN connectors

- Amazon Web Services
- Cisco Application Centric Infrastructure
- Google Cloud Platform
- Microsoft Azure
- Nuage Virtualized Services Platform
- Oracle Cloud Infrastructure
- VMware NSX

SSO/identity connectors

- Poll Active Directory server
- RADIUS single sign-on agent
- Fortinet single sign-on agent

Threat feed connectors

- FortiGuard category
- Firewall IP address
- Domain name

If your FortiGate has VDOMs enabled, SDN and threat feed connectors are global settings, while SSO/identity connectors are available per-VDOM.

Configuring Fabric Connectors

The method that you use to configure a Fabric Connector depends on which type of connector you're using:

- Creating an SDN Connector
- Creating an SSO Connector
- Creating a Threat Feed Connector

Creating an SDN Connector

FortiOS doesn't support multiple SDN Connector instances to Amazon Web Services, Google Cloud Platform, Microsoft Azure, and VMware NSX.

Software-Defined Network (SDN) Connectors provide integration and orchestration of Fortinet products with key SDN solutions. You use SDN Connectors to make sure that any changes in your SDN environment are automatically updated in your network.

To create an SDN Connector, you need to do the following:

- Gather required information
- Create the Fabric Connector
- Create a Fabric Connector address
- Add the address to a firewall policy

For an example of how to configure a Fabric Connector for Microsoft Azure, see FortiGate SDN Connector for Azure.

Gather required information

Before you can create an SDN Connector, you need to know specific information, which differs depending on which service you're using. You can find this information using your account for the specific service.

Service	Required information for the service
Amazon Web Services	• Access key ID • Secret access key • Region name • VPC ID (optional)

Service	Required information for the service
Cisco Application Centric Infrastructure	• IP address • Port • Username • Password
Google Cloud Platform	• Project name • Service account email • Private key
Microsoft Azure	• Tenant ID • Client ID • Client secret • Subscription ID (optional) • Resource group (optional)
Nuage Virtualized Services Platform	• IP address • Port • Username • Password
Oracle Cloud Infrastructure	• User ID • Tenant ID • Compartment ID • Server region • Certificate
VMware NSX	• IP address or hostname • Username • Password

Create the Fabric Connector

You can create the Fabric Connector using either the GUI or CLI. The CLI commands that are available vary depending on which service you're using.

Creating a Fabric Connector - GUI:

1. To create a new connector, go to **Security Fabric > Fabric Connectors** and select **Create New**.
2. Select the service you're using and enter the required information for that service.
3. Select **OK**.

Creating a Fabric Connector - CLI:

To create a Fabric Connector using the CLI, use the command `config system sdn-connector`. For more information about this command, see the FortiOS 6.0 CLI Reference.

Create a Fabric Connector address

You use a Fabric Connector address for the following:

- As the source or destination address for firewall policies
- To automatically update changes to the addresses in the environment of the service you're using, based on specified filtering conditions
- To automatically apply changes to the firewall policies that use the address, based on specified filtering conditions

Creating a Fabric Connector address - GUI:

1. To create a new address, go to **Policy & Objects > Addresses** and select **Create New > Address**.
2. Set a **Name** for the address.
3. Set **Type** to **Fabric Connector Address** and set **Fabric Connector Type** to the appropriate service.
4. Set a **Filter**. This filter dynamically creates the members of the address. The types of filters that are supported vary depending on which service you're using.
5. Set a specific **Interface** or leave it as the default **any**.
6. Select **OK**.

Creating a Fabric Connector address - CLI:

```
config firewall address
   edit <name>
      set type dynamic
      set comment <comment>
      set visibility enable
      set associated-interface <interface_name>
      set sdn {aci | aws | azure | nsx | nuage | oci}
      set filter <filter>
   next
end
```

Add the address to a firewall policy

You use a Fabric Connector addresses in a firewall policy as either the source or destination address.

Adding the address to a policy - GUI:

1. To create a new policy, go to **Policy & Objects > IPv4 Policy** and select **Create New**.
2. Set a **Name** for the policy.
3. Set the appropriate **Incoming Interface** and **Outgoing Interface**.
4. Set the Fabric Connector address as either the **Source** or **Destination** address, as appropriate.
5. Set other policy settings, as required.
6. Select **OK**.

Adding the address to a policy - CLI:

```
config firewall policy
   edit 0
      set name <name>
      set srcintf <port_name>
      set dstintf <port_name>
      set srcaddr <firewall_address>
      set dstaddr <firewall_address>
      set action accept
      set schedule <schedule>
      set service <service>
   next
end
```

Creating an SSO Connector

SSO Connectors integrate single sign-on (SSO) authentication in your network. SSO allows users to enter their credentials once and have those credentials reused when they access other network resources through your FortiGate.

Connectors are available for the following services:

- Poll Active Directory (AD) server
- RADIUS Single Sign-On (RSSO) agent
- Fortinet Single Sign-On (FSSO) agent

For more information about SSO Connectors, see the Authentication Handbook.

Creating a Threat Feed Connector

Threat Feed Connectors dynamically import an external block list, in the form of a text file containing a list of either addresses or domains, which resides on an HTTP server. You use block lists to deny access to source or destination IP addresses in web filter and DNS filter profiles, SSL inspection exemptions, and as sources or destinations in proxy policies.

You can configure the following types of threat feeds:

- FortiGuard category
- IP address
- Domain name

For more information about Threat Feed Connectors, see the Security Profiles Handbook.

Verifying Fabric Connector status

You can only verify the status for Fabric Connectors to AWS, Microsoft Azure, OCI, and VMware NSX.

To verify the status of a Fabric Connector, use one of the following commands:

- `diagnose system sdn status` to verify all connectors
- `diagnose system sdn status <connector_name>` to verify a specific connector

After you enter the command, one of four statuses is displayed:

- `connected`: the connector is connected
- `not connected`: the connector isn't connected
- `disabled`: the related connector entry is set to disabled
- `unknown`: verification of the connector isn't supported

Example output

```
# diagnose sys sdn status
SDN Connector Type Status
------------------------------------------------------------
aci-sdn-connector aci unknown
aws-sdn-connector aws disabled
azure-sdn-connector azure not connected
nsx-sdn-connector nsx connected
```

Central management with FortiManager

This section describes the basics of using FortiManager as an administration tool for multiple FortiGate devices. It describes the key management features you can use to manage a FortiGate in FortiManager. It contains the following sections:

- Configuring the FortiManager
- FortiGuard
- Firmware updates
- Administrative domains
- Backing up and restoring configurations
- FortiManager in backup mode

For more information about FortiManager, see the FortiManager Administration Guide.

For the FortiGate and the FortiManager to connect properly, both devices must have compatible firmware. To find out if your firmware is compatible, see the FortiOS Release Notes and FortiManager Release Notes.

Configuring the FortiManager

For information about configuring the connection between your FortiGate devices and FortiManager, see "Adding a FortiManager to the Security Fabric" on page 26.

After you configure the connection between your FortiGate devices and FortiManager, you can configure the following items on the FortiManager:

- Configuring updates through FortiManager
- Using global objects
- Locking the FortiGate GUI
- SSL connections

Configuring updates through FortiManager

With the FortiManager system, you can monitor and configure multiple FortiGate devices from one location. You can use the FortiManager Device Manager to view FortiGate devices and make the usual configuration updates and changes, without logging in and out of multiple FortiGate devices.

FortiManager allows you to complete the configuration by going to the Device Manager, selecting the FortiGate, and using the same menu structure and pages as you see in the FortiGate GUI. All changes to the FortiGate configuration are stored locally on the FortiManager until you synchronize with the FortiGate.

When a FortiGate is under the control of a FortiManager device, you shouldn't use the FortiGate to change the configuration. When you try to change options, the FortiGate displays a message stating that it's configured through FortiManager and any changes may be reverted.

Central management configuration supports multiple FortiManager addresses, which helps mainly in the case where the FortiGate is behind NAT.

Using global objects

If you maintain several FortiGate devices within a network, many of the policies and configuration elements are the same across your organization. You can use FortiManager global objects to simplify policy configuration for the FortiGate devices in the network so that you don't have to add and edit many of the same policies on each FortiGate device.

A global object is an object that isn't associated with one device or group. Global objects include security policies, a DNS server, VPNs, and IP pools. You can copy the configurations to the FortiManager device database for a selected device or group of devices. You can also import configurations from the FortiManager device database for a selected device and modify the configuration, as required. When you configure or create a global policy object, the interface, prompts, and fields are the same as creating the same object on a FortiGate using the FortiGate GUI.

Locking the FortiGate GUI

When you use the FortiManager to manage multiple FortiGate devices, a local FortiGate is locked and most administrators are prevented from making configuration changes, using the GUI. The super_admin can still make changes to the configuration, but this isn't recommended since it may cause conflicts with the FortiManager.

SSL connections

An SSL connection can be configured to encrypt traffic between FortiManager and the FortiGate devices.

Configuring an SSL connection

Use the following CLI commands in the FortiGate CLI to configure the connection:

```
config system central-management
   set status enable
   set enc-algorithm {default* | high | low}
end
```

The default encryption automatically sets high and medium encryption algorithms. Algorithms used for high, medium, and low follows openssl definitions:

- **High** - Key lengths larger than 128 bits, and some cipher suites with 128-bit keys.

Algorithms are: DHE-RSA-AES256-SHA:AES256-SHA: EDH-RSA-DES-CBC3-SHA: DES-CBC3-SHA:DES-CBC3-MD5:DHE-RSA-AES128-SHA:AES128-SHA

- **Medium** - Key strengths of 128 bit encryption.

Algorithms are: RC4-SHA:RC4-MD5:RC4-MD

- **Low** - Key strengths of 64 or 56 bit encryption algorithms but excluding export cipher suites

Algorithms are: EDH-RSA-DES-CDBC-SHA; DES-CBC-SHA; DES-CBC-MD5.

Enable / disable logging of SSL connection events

The following commands allow the user to enable or disable logging of SSL connection events. The default is `disable`.

Syntax

```
config system global
   set log-ssl-connection {enable | disable}
end
```

Enabling or disabling static key ciphers (379616)

The following CLI commands under `system global` let you enable or disable static key ciphers in SSL/TLS connections (e.g,. AES128-SHA, AES256-SHA, AES128-SHA256, AES256-SHA256). The default is `enable`.

Syntax

```
config system global
   set ssl-static-key-ciphers{enable | disable}
end
```

FortiGuard

The FortiGuard Distribution Network (FDN) provides FortiGuard services for the FortiManager system and its managed devices and FortiClient agents. The FDN is a world-wide network of FortiGuard Distribution Servers (FDS), which update the FortiGuard services on your FortiManager system on a regular basis so that your FortiManager system is protected against the latest threats.

This section contains the following:

- Setting up FortiGuard
- Configuring FortiGuard licensing for devices with limited or no connectivity
- Troubleshooting your FortiGuard connection

Setting up FortiGuard

In FortiGuard Management, you can configure the FortiManager system to act as a local FDS, or use a web proxy server to connect to the FDN. FortiManager systems acting as a local FDS synchronize their FortiGuard service update packages with the FDN, then provide these updates and look up replies to the FortiGate devices in your private network. The local FDS provides a faster connection, which reduces the Internet connection load and the time that's required to apply frequent updates, such as antivirus signatures, to many devices.

The default port that's used for FortiGuard services is UDP/8888.

The FortiManager system includes the following FortiGuard services:

- Antivirus and IPS engines and signatures (including mobile malware)
- Web filtering and email filtering rating databases and lookups (select systems)
- Vulnerability scan and management support for FortiAnalyzer

To view and configure these services, go to **FortiGuard > Settings** on the FortiManager.

FortiManager can also connect to the FortiGuard Distribution Network (FDN) to receive push updates for IPS signatures and antivirus definitions. These updates can then be used to update multiple FortiGate devices throughout your organization. By using the FortiManager as the host for updates, bandwidth use is minimized as updates are downloaded to one source instead of many.

To receive IPS and antivirus updates from FortiManager, indicate an alternate IP address on the FortiGate.

To configure updates from FortiManager - GUI:

1. In the FortiGate GUI, go to **System > FortiGuard**.
2. Under **AntiVirus & IPS Updates**, enable both **Accept push updates** and **Use override push**.
3. Enter the IP address of the FortiManager.
4. Select **Apply**.

The FortiManager can also operate as a local FDS server when it's in a closed network with no Internet connectivity. For more information, see "Configuring FortiGuard licensing for FortiGate devices with limited or no connectivity" on page 1.

Extended database version OIDs for AV and IPS

New extended database version OIDs ensure accurate display of the AntiVirus and IPS databases in use when you go to **System > FortiGuard**.

IPS signatures page

The IPS signatures list page shows which IPS package is currently deployed. You can change the IPS package by hovering over the information icon next to the IPS package name. Text appears that links directly from the IPS signatures list page to the **System > FortiGuard** page on the FortiGate.

The central management FortiGuard server list can include FQDNs

This feature implements support for FQDN, to make it an option for central-management server-list.

To add FQDN as an address type - GUI:

On **System > FortiGuard > Override FortiGuard Servers > Create New / Edit**, an **FQDN** option, is added for **Address Type**.

CLI changes

```
config server-list
   edit 1
      set server-type {update | rating}
      set addr-type {ipv4 | ipv6 | fqdn} <== added fqdn
      set server-address ipv4
      set server-address6 ipv6
      set fqdn FQDN <== added
   end
end
```

Sending malware statistics to FortiGuard

To support following malware trends and making zero-day discoveries, FortiGate devices send encrypted statistics to FortiGuard about IPS, application control, and antivirus events that FortiGuard services running on the FortiGate detect. FortiGuard uses the statistics collected to achieve a balance between performance and security effectiveness by moving inactive signatures to an extended signature database.

The statistics include some non-personal information that identifies the FortiGate and its country. This information is never shared with external parties. You can choose to disable the sharing of this information by entering the following CLI command:

```
config system global
   set fds-statistics disable
end
```

Configuring FortiGuard licensing for devices with limited or no connectivity

In some high security environments, Internet service from internal FortiGate devices or for the FortiManager is restricted. This section describes how to configure devices with limited or no internet connectivity to receive FortiGuard updates.

Preliminary steps

1. Register the FortiGate. For a physical FortiGate, use the serial number. For a FortiGate virtual machine (VM), use the registration number. To register the FortiGate, visit the Fortinet Support website.
2. For FortiGate VMs, the registration process creates a unique license file that's available under **Asset > View/Manage Products**. Select the correct device and download the license file.

This section assumes that:

- Internal FortiGate devices can access a local physical FortiManager or FortiManager VM.
- The FortiManager is running firmware version 6.0.0 or later.

After you have completed the following steps, use the following instructions:

- Configuring a FortiGate without Internet connectivity to access a local FortiManager as FDN
- Configure FortiManager without Internet connectivity as a local FDN server

Configuring a FortiGate without Internet connectivity to access a local FortiManager as FDN

By default, FortiGate connects to the public FDN to validate its license and download security feature updates, including databases and engines for security feature updates, such as AntiVirus and IPS. You can configure a FortiGate to use a local FortiManager for both license validation and FDN updates.

For a FortiGate that doesn't have Internet access, you must complete the full configuration before you upload the license. When the FortiGate receives a license file (from the GUI or CLI), it immediately attempts to access the public FDN to validate the license. Until the license is validated, you can't log in to the GUI and some CLI commands aren't available, including the commands that you need to define a local FDN server. This makes it very difficult for you to add the necessary commands to point the FortiGate to a local FortiManager to validate the license.

This document describes how to configure a FortiGate for local FDN access, and provides you with a workaround to fix a FortiGate that can't access a public license validation server.

Follow this procedure to configure a FortiGate to use a local FortiManager for FDN access.

If you complete these steps in a different order, the process may fail, and the FortiGate won't be able to validate the license.

In the FortiGate CLI:

1. Configure central management settings:

```
config system central-management
   config server-list
      edit 1
         set server-type update rating
         set server-address <fortimanager_ip>
      next
   end
   set include-default-servers disable
end
```

2. Upload the license using TFTP:

```
execute restore vmlicense tftp <filename>.lic <tftp_ip>
```

   The FortiGate reboots.

3. Complete the central management configuration:

```
config system central-management
   set fmg <fortimanager_ip>
end
```

In the FortiManager GUI:

You must manually add devices to the FortiManager.

As a result of the CLI commands that you entered on the FortiGate, the device is displayed in the FortiManager GUI, in the **Unregistered Devices** list that's located in the **Device Manager** pane for the root ADOM.

When you enable ADOMs, you must assign the device to an ADOM when you register it.

To add devices manually:

1. Confirm that central management is enabled for the device (as above).
2. In FortiManager, select the root ADOM, and go to **Device Manager**.
3. In the tree menu, click **Unregistered Devices**. The content pane displays the unregistered devices.
4. Select the unregistered device or devices, then click **Add**.
   The **Add Device** dialog box opens.
5. If ADOMs are enabled, select the ADOM in the **Add the following device(s) to ADOM** list. If ADOMs are disabled, select **root**.
6. Type the login and password for each device.
7. Click **OK** to register the devices.

The devices are added.

Configure FortiManager without Internet connectivity as a local FDN server

The FortiManager can be operated as a local FDS server when it is in a closed network with no Internet connectivity.

Without a connection to a FortiGuard server, update packages and licenses must be manually downloaded from support, and then uploaded to the FortiManager. Through this feature, known as **Closed Network Mode**, the FortiManager can then provide updates and validate licenses for local FortiGate devices without Internet access.

To configure the FortiManager in Closed Network Mode, complete the following tasks:

- Enable Closed Network Mode
- Request FortiGate license validation information
- Download FortiGuard service update files
- Configure FortiManager in Closed Network Mode

Enable Closed Network Mode

1. From the FortiManager GUI, go to **FortiGuard > Settings** and disable **Enable Communication with FortiGuard Server**.
   Or, from the FortiManager CLI, enable Closed Network Mode by disabling FDS access from the public FDN:

```
config fmupdate publicnetwork
  set status disable
end
```

Once in Closed Network Mode, you must manually import FortiManager service packages, updates, and license upgrades.

Request FortiGate license validation information

1. Create a Customer Service ticket with Fortinet Support under **Assistance > Create Ticket > Customer Service > Submit Ticket**.
2. Enter the serial number. Under **Category**, select **CS Contract/License**.
3. In the **Comment** field, ask for an "entitlement file" for the FortiGate. Provide the serial number and license number available in **Asset > Manage/View Products >**<Select product>.
   Example:
   Serial Number: FGVM010000024628
   License Number: FGVM0035444

As with asset registration, for large numbers of FortiGate devices you can attach a spreadsheet of serial and license numbers for Customer Service. They will provide a single entitlement file that contains validation information for all FortiGate devices in the spreadsheet. All FortiGate devices must be registered under the same account. Devices registered under different accounts cannot be combined into the same entitlement file.

4. You will receive an entitlement file from Customer Service.

Download FortiGuard service update files

1. From Fortinet Support, navigate to **Download > FortiGuard Service Updates**. Download the **Virus Definition**, **Attack Definition**, and **Mobile Malware** files for the appropriate version of FortiGate and FortiOS. These files are named in the form vsigupdate*.pkg and nids*.pkg.
2. Export the FortiGuard Web Filter and Anti-Spam service updates from a FortiManager that has Internet connectivity by entering the following CLI command:

```
execute fmupdate {ftp | scp | tftp} export <type> <remote_file> <ip> <port>
    <remote_path> <user> <password>
```

Enter types `url` and `spam`.

Variable	Description
`{ftp | scp | tftp}`	Select the file transfer protocol to use: ftp, scp, or tftp.
`<type>`	Select the type of file to export or import. The following options are available: `av-ips`, `fct-av`, `url`, `spam`, `file-query`, `license-fgt`, `license-fct`, `custom-url`, or `domp`.
`<remote_file>`	Update manager packet file name on the server or host.
`<ip>`	Enter the FQDN or the IP address of the server.
`<port>`	Enter the port to connect to on the remote SCP host. Range: 1 to 65535 .
`<remote_path>`	Enter the name of the directory of the file to download from the FTP server or SCP host. If the directory name has spaces, use quotes instead.
`<user>`	Enter the user name to log into the FTP server or SCP host.
`<password>`	Enter the password to log into the FTP server or SCP host.

Configure FortiManager in Closed Network Mode

Go to **FortiGuard > Settings** to configure FortiManager as a local FDS server and to upload update packages and licenses.

1. Toggle **OFFEnable Communication with FortiGuard Server** to disable communication with the FortiGuard servers.
2. Toggle **ONEnable Antivirus and IPS Service**.
   Select software versions for FortiGate, FortiClient, FortiAnalyzer, and FortiMail.
3. Toggle **ONEnable Web Filter Service**.
   When uploaded to FortiManager, the Web Filter database is displayed.
4. Toggle **ONEnable Email Filter Service**.
   When uploaded to FortiManager, the Email Filter database is displayed.

5. Under **Upload Options for FortiGate/FortiMail**
   - Upload **AntiVirus/IPS Packages**. Browse for the file you downloaded from the Customer Service Support portal on your management computer. Select **OK** to upload the package to FortiManager. Repeat for each file downloaded from the Customer Service Support portal.
   - Upload **Web Filter Database**. Browse for the file you exported from the FortiManager that is connected to the Internet. Select **OK** to upload the package to FortiManager in the closed network mode. As the database can be large, uploading with the CLI is recommended. See the instructions below.
   - Upload **Email Filter Database**. Browse for the file you exported from the FortiManager that is connected to the Internet. Select **OK** to upload the package to FortiManager in closed network mode. As the database can be large, uploading with the CLI is recommended. See the instructions below.
   - Select **Service License** to import the FortiGate license. Browse for the entitlement file on your management computer. Select **OK** to upload the package to FortiManager. A license file can be obtained from support by requesting your account entitlement for the device (see "Configuring FortiGuard licensing for devices with limited or no connectivity" on page 65).
6. Under **Upload Options for FortiClient**, select **AntiVirus/IPS Packages** to upload the FortiClient AntiVirus/IPS packages. Browse for the file downloaded from the Customer Service & Support portal on your management computer. Select **OK** to upload the package to FortiManager.

Uploading packages with the CLI

You can upload packages and licenses with the CLI. You should use this method when packages are large, such as database packages.

First, disable communications with the FortiGuard server and enable a closed network with the following CLI commands:

```
config fmupdate publicnetwork
   set status disable
end
```

Then, upload an update package or license by loading the package or license file to an FTP, SCP, or TFTP server.

Run the following CLI command:

```
execute fmupdate { ftp | scp | tftp } import < av-ips | fct-av | url | spam | file-query |
    license-fgt | license-fct | custom-url | domp > <remote_file> <ip> <port> <remote_
    path> <user> <password>
```

Troubleshooting your FortiGuard connection

You can use the following commands to determine the state of license validation and FDN service connectivity, and gather information about connectivity failures. For more information about troubleshooting commands, see the FortiOS CLI Reference.

On a FortiGate, use the following commands:

- `get system status`
- `get webfilter status`
- `get system auto-update version`
- `get system auto-update status`

On a FortiGate VM, use the following commands:

- `diagnose hardware sysinfo vm full`
- `diagnose debug vm-print-license`
- `diagnose hardware sysinfo vminfo`

On a FortiManager, use the following commands:

- `diagnose fmupdate vm-license`

Firmware updates

A FortiManager can also perform firmware updates for multiple FortiGate devices which saves you time because you don't have to upgrade each FortiGate individually.

The FortiManager stores local copies of firmware images, when it downloads images from the Fortinet Distribution Network (FDN) or accepts firmware images that you upload from the management computer.

If you use the FortiManager to download firmware images, the FDN first validates device licenses and support contracts and then provides a list of firmware images that are currently available. For devices with valid Fortinet Technical Support contracts, you can download new firmware images from the FDN and the firmware release notes. After firmware images are downloaded, you can either schedule or immediately upgrade or downgrade the firmware for a device or a group of device.

For more information about updating the FortiGate firmware using FortiManager central management, see the FortiManager Administration Guide.

Administrative domains

FortiManager administrative domains allow the super_admin to create groupings of devices for configured administrators to monitor and manage. FortiManager can manage a large number of Fortinet appliances. This allows you to maintain managed devices that are specific to their geographic location or business division. This also includes FortiGate devices with multiple VDOMs.

Each administrator is tied to an administrative domain (ADOM). When the administrator logs in, they see only those devices or VDOMs that are configured for that administrator and ADOM. The one exception is the super_admin account that can see and maintain all administrative domains and the devices within those domains.

Administrative domains aren't enabled by default and only the super_admin can enable and configure the domains.

The maximum number of administrative domains you can add depends on the FortiManager system model. For more information about the maximums for each model, see the FortiManager Administration Guide.

Backing up and restoring configurations

A FortiManager stores configuration files for backup and restore purposes. A FortiManager also allows you to save revisions of configuration files. Configuration backups occur automatically when you log out or the

administrator login session expires.

FortiManager also allows you to view differences between different configurations so that you can identify where changes have been made.

FortiManager in backup mode

Running a FortiManager ADOM in backup mode allows you to use the FortiManager as a central database for address and service objects which are common across multiple devices that are connected to that ADOM. When a FortiManager ADOM is in backup mode, the FortiManager administrator is responsible for managing the database but not the FortiGate configurations.

FortiGate administrators are responsible for making changes to FortiGate devices. When changes are made, the FortiGate administrator is notified of any new, updated, or out-of-sync objects. The administrator can import or update these objects, as needed.

When the FortiManager is in backup mode, the FortiGate configuration is synchronized on demand with FortiManager, similar to how it is done in normal mode and keeps the FortiManager and FortiGate closely synchronized.

Backup mode is useful when you have networks in multiple locations, each with their own administrators who require the ability to make changes quickly.

To add a FortiManager in backup mode, you must first configure an ADOM on the FortiManager that is in backup mode. You can then add the FortiGate to that ADOM using the **Central Management** settings, found at **Security Fabric > Settings**. Make sure to set **Mode** to **Backup**.

To access shared objects from the FortiManager, select the Central Management icon in the GUI header and select **View Details**. A menu opens, showing all FortiManager objects, with options to import, update, or delete objects as necessary.

Related resources

Document	Location
Security Fabric documentation	http://docs.fortinet.com/security-fabric/admin-guides
The Security Fabric Cookbook Recipe Collection	http://cookbook.fortinet.com/security-fabric-collection-60/
Security Fabric Upgrade Guide	https://docs.fortinet.com/security-fabric/release-information
Fortinet Communication Ports and Protocols Guide	https://docs.fortinet.com/fortigate/reference
FortiGate documentation	http://docs.fortinet.com/fortigate/admin-guides
FortiAnalyzer documentation	http://docs.fortinet.com/fortianalyzer/admin-guides
FortiAP documentation	http://docs.fortinet.com/fortiap/admin-guides
FortiClient documentation	http://docs.fortinet.com/forticlient/admin-guides
FortiClient EMS documentation	http://docs.fortinet.com/ems/admin-guides
FortiMail documentation	http://docs.fortinet.com/fortimail/admin-guides
FortiManager documentation	http://docs.fortinet.com/fortimanager/admin-guides
FortiSandbox documentation	http://docs.fortinet.com/fortisandbox/admin-guides
FortiSwitch documentation	http://docs.fortinet.com/fortiswitch/admin-guides
FortiWeb documentation	http://docs.fortinet.com/fortiweb/admin-guides